Open Source Used In IOS XR Software 7.0.14

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Text Part Number: 78EE117C99-1077740443

This document contains licenses and notices for open source software used in this product. With respect to the free/open source software listed in this document, if you have any questions or wish to receive a copy of any source code to which you may be entitled under the applicable free/open source license(s) (such as the GNU Lesser/General Public License), please submit this form.

In your requests please include the following reference number 78EE117C99-1077740443

Contents

1.1 grub 0.97
1.1.1 Available under license
1.2 csrp 1.0
1.2.1 Available under license
1.3 sed 4.2.2
1.3.1 Available under license
1.4 xinetd 2.3.15
1.4.1 Available under license
1.5 bzip2 1.0.6
1.5.1 Available under license
1.6 binutils 2.24
1.6.1 Available under license
1.7 python 3.5.1
1.7.1 Available under license
1.8 dbus-glib 0.106
1.8.1 Available under license
1.9 findutils 4.6.0
1.9.1 Available under license
1.10 dhcp 4.3.4
1.10.1 Available under license
1.11 openssl 1.0.2j
1.11.1 Notifications
1.11.2 Available under license
1.12 libxslt 1.1.29
1.12.1 Available under license
1.13 glib 2.48.2

1.13.1 Available under license
1.14 glibc 2.24
1.14.1 Available under license
1.15 python 2.7.12
1.15.1 Available under license
1.16 openssh 7.3p1
1.16.1 Available under license
1.17 gnutls 3.5.3
1.17.1 Available under license
1.18 libarchive 3.2.2
1.18.1 Available under license
1.19 libpng 1.6.24
1.19.1 Available under license
1.20 m4 1.4.17
1.20.1 Available under license
1.21 dropbear 2016.74
1.21.1 Available under license
1.22 inetutils 1.9.4
1.22.1 Available under license
1.23 ntp 4.2.8p10
1.23.1 Available under license
1.24 sqlite 3.23.1
1.24.1 Available under license
1.25 libtool 2.4.6
1.25.1 Available under license
1.26 libusb 1.0.20
1.26.1 Available under license
1.27 libyaml 0.1.7
1.27.1 Available under license
1.28 ncurses 6.0
1.28.1 Available under license
1.29 libidn 1.33
1.29.1 Available under license
1.30 zlib 1.2.3
1.30.1 Available under license
1.31 zlib 1.2.8
1.31.1 Available under license
1.32 gawk 4.1.3
1.32.1 Available under license

1.33 coreutils 8.25
1.33.1 Available under license
1.34 cpio 2.12
1.34.1 Available under license
1.35 e2fsprogs 1.43
1.35.1 Available under license
1.36 patch 2.7.5
1.36.1 Available under license
1.37 ebtables 2.0.10
1.37.1 Available under license
1.38 libevent 2.1.8
1.38.1 Available under license
1.39 libtirpc 1.0.1
1.39.1 Available under license
1.40 avahi 0.6.32
1.40.1 Available under license
1.41 i2c-tools 3.1
1.41.1 Available under license
1.42 parted 3.2
1.42.1 Available under license
1.43 grub 2.02
1.43.1 Available under license
1.44 iconv 2.24
1.44.1 Available under license
1.45 libgcrypt 1.7.3
1.45.1 Available under license
1.46 fuse 2.9.4
1.46.1 Available under license
1.47 lighttpd 1.4.41
1.47.1 Available under license
1.48 gnupg 2.1.14
1.48.1 Available under license
1.49 harfbuzz 1.3.0
1.49.1 Available under license
1.50 bash 4.3.47
1.50.1 Available under license
1.51 cairo 1.14.6
1.51.1 Available under license
1.52 ethtool 4.6

1.52.1 Available under license
1.53 libsodium 1.0.1
1.53.1 Available under license
1.54 libassuan 2.4.3
1.54.1 Available under license
1.55 grep 2.25
1.55.1 Available under license
1.56 lxc 2.0.4
1.56.1 Available under license
1.57 nspr 4.12
1.57.1 Available under license
1.58 wget 1.18
1.58.1 Available under license
1.59 sudo 1.8.17
1.59.1 Available under license
1.60 tcl 8.6.6
1.60.1 Available under license
1.61 gpgme 1.10.0
1.61.1 Available under license
1.62 lvm2 2.02.166
1.62.1 Available under license
1.63 elfutils 0.166
1.63.1 Available under license
1.64 tcl 8.3.2
1.64.1 Available under license
1.65 jansson 2.9
1.65.1 Available under license
1.66 libdaemon 0.14
1.66.1 Available under license
1.67 busybox 1.24.1
1.67.1 Available under license
1.68 gdb 7.10.1
1.68.1 Available under license
1.69 net-tools 1.60
1.69.1 Available under license
1.70 libnss-mdns 0.10
1.70.1 Available under license
1.71 libgpg-error 1.24
1.71.1 Available under license

1.72 zeromq 4.1.5
1.72.1 Available under license
1.73 sqlite 3.14.1
1.73.1 Available under license
1.74 libxml 2.9.4
1.74.1 Available under license
1.75 pixman 0.34.0
1.75.1 Available under license
1.76 libnih 1.0.3
1.76.1 Available under license
1.77 gmp 6.1.1
1.77.1 Available under license
1.78 libnet 1.2
1.78.1 Available under license
1.79 linux-kernel 4.10.17
1.79.1 Available under license
1.80 fontconfig 2.12.1
1.80.1 Available under license
1.81 linux-kernel 4.8.28
1.81.1 Available under license
1.82 jansson 2.7
1.82.1 Available under license
1.83 file 5.27
1.83.1 Available under license
1.84 libpcap 1.7.4
1.84.1 Available under license
1.85 cronie 1.5.1
1.85.1 Available under license
1.86 diffutils 3.4
1.86.1 Available under license
1.87 libcheck 0.10.0
1.87.1 Available under license
1.88 libpciaccess 0.13.4
1.88.1 Available under license
1.89 bind 9.11.6
1.89.1 Available under license
1.90 cryptsetup 1.7.2
1.90.1 Available under license
1.91 libnftnl 1.0.6

1.91.1 Available under license
1.92 procps 3.3.12
1.92.1 Available under license
1.93 tar 1.29
1.93.1 Available under license
1.94 perl 5.22.1
1.94.1 Available under license
1.95 tcpdump 4.7.4
1.95.1 Available under license
1.96 xz 5.2.2
1.96.1 Available under license
1.97 at 3.1.20
1.97.1 Available under license
1.98 libvirt 1.3.5
1.98.1 Available under license
1.99 fdisk 2.28.1
1.99.1 Available under license
1.100 curl 7.30.0
1.100.1 Available under license
1.101 strace 4.13
1.101.1 Available under license
1.102 expat 2.2.0
1.102.1 Available under license
1.103 expat 2.1.0
1.103.1 Available under license
1.104 rsync 3.1.2
1.104.1 Available under license
1.105 shadow 4.2.1
1.105.1 Available under license
1.106 perl 5.20.0
1.106.1 Available under license
1.107 dnsmasq 2.76
1.107.1 Available under license
1.108 expat 2.1.1
1.108.1 Available under license
1.109 log-rotate 3.9.1
1.109.1 Available under license
1.110 libksba 1.3.4
1.110.1 Available under license

1.111 util-linux 2.28.1
1.111.1 Available under license
1.112 d-bus 1.10.10
1.112.1 Available under license
1.113 expat 2.2.8
1.113.1 Available under license
1.114 avahi 0.7
1.114.1 Available under license
1.115 netcat 0.7.1
1.115.1 Available under license
1.116 openssl 1.0.2r
1.116.1 Available under license
1.117 libnl3 3.2.28
1.117.1 Available under license
1.118 golang 1.8.1
1.118.1 Available under license
1.119 efivar 0.24
1.119.1 Available under license
1.120 policycoreutils 2.6
1.120.1 Available under license
1.121 sysklogd 1.5.1
1.121.1 Available under license
1.122 base-passwd 3.5.3
1.122.1 Available under license
1.123 ipmi-tool 1.8.15
1.123.1 Available under license
1.124 u-boot 2016.07
1.124.1 Available under license
1.125 mbed-tls TLS 2.6.0
1.125.1 Available under license
1.126 libssh2 1.7.0
1.126.1 Available under license
1.127 zstd 1.33
1.127.1 Available under license
1.128 gdbm 1.12
1.128.1 Available under license
1.129 psmisc 22.21
1.129.1 Available under license
1.130 pciutils 3.5.1

1.130.1 Available under license
1.131 libsepol 2.6
1.131.1 Available under license
1.132 flex 2.6.0
1.132.1 Available under license
1.133 efibootmgr 0.12
1.134 libsemanage-common 2.6
1.134.1 Available under license
1.135 libedit 20150325-3.1
1.135.1 Available under license
1.136 dmidecode 3.5
1.136.1 Available under license
1.137 pinentry 0.9.2
1.137.1 Available under license
1.138 berkeley-db 6.0.35
1.138.1 Available under license
1.139 npth 1.2
1.139.1 Available under license
1.140 hd-parm 9.56
1.140.1 Available under license

1.1 grub 0.97

1.1.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our
General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer
you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND
CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below,

refers to any such program or work, and a "work based on the Program"
means either the Program or any derivative work under copyright law:
that is to say, a work containing the Program or a portion of it,
either verbatim or with modifications and/or translated into another
language. (Hereinafter, translation is included without limitation in
the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not
covered by this License; they are outside its scope. The act of
running the Program is not restricted, and the output from the Program
is covered only if its contents constitute a work based on the
Program (independent of
having been made by running the Program).
Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's
source code as you receive it, in any medium, provided that you
conspicuously and appropriately publish on each copy an appropriate
copyright notice and disclaimer of warranty; keep intact all the
notices that refer to this License and to the absence of any warranty;
and give any other recipients of the Program a copy of this License
along with the Program.

You may charge a fee for the physical act of transferring a copy, and
you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion
of it, thus forming a work based on the Program, and copy and
distribute such modifications or work under the terms of Section 1
above, provided that you also meet all of these conditions:

a) You must cause the modified
files to carry prominent notices
stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in
whole or in part contains or is derived from the Program or any
part thereof, to be licensed as a whole at no charge to all third
parties under the terms of this License.

c) If the modified program normally reads commands interactively
when run, you must cause it, when started running for such
interactive use in the most ordinary way, to print or display an
announcement including an appropriate copyright notice and a
notice that there is no warranty (or else, saying that you provide
a warranty) and that users may redistribute the program under
these conditions, and telling the user how to view a copy of this
License. (Exception: if the Program itself is interactive but

does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source

code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component

itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program
or its derivative works. These actions are
prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order,
agreement or
otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot

distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software

Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) 19yy <name of author>

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation; either version 2 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program;
if not, write to the Free Software
Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19yy name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than 'show w' and 'show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright
disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
'Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the

library. If this is what you want to do, use the GNU Library General
Public License instead of this License.

1.2 csrp 1.0

1.2.1 Available under license :

Copyright (c) 2010, Tom Cocagne
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright
  notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.
* Neither the name of the Python Software Foundation nor the
  names of its contributors may be used to endorse or promote products
  derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 PURPOSE ARE
DISCLAIMED. IN NO EVENT SHALL TOM COCAGNE BE LIABLE FOR ANY
DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES
(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND
ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

1.3 sed 4.2.2

1.3.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for
software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software,
we are referring to freedom, not
price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL
protect your rights with two steps:
(1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If

such problems arise substantially in other domains, we
stand ready to extend this provision to those domains in future versions
of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents.
States should not allow patents to restrict development and use of
software on general-purpose computers, but in those that do, we wish to
avoid the special danger that patents applied to a free program could
make it effectively proprietary. To prevent this, the GPL assures that
patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and
modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of
works, such as semiconductor masks.

"The Program" refers to any copyrightable work
licensed under this
License. Each licensee is addressed as "you". "Licensees" and
"recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work
in a fashion requiring copyright permission, other than the making of an
exact copy. The resulting work is called a "modified version" of the
earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based
on the Program.

To "propagate" a work means to do anything with it that, without
permission, would make you directly or secondarily liable for
infringement under applicable copyright law, except executing it on a
computer or modifying a private copy. Propagation includes copying,
distribution (with or without modification), making available to the
public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other
parties to make or receive
copies. Mere interaction with a user through
a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified
for a particular programming language, one that
is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including
scripts to
control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding

Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions
are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted
material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological

measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving
a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation
of a covered work with other separate and independent
works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an

"aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the

Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a

requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation
available to the public in
source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions
on material, added by you to a covered work,
for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation
of a covered work
occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an
entity transaction, each party to that
transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation

(including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the
business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you
from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this

License will continue to apply to the part which is the covered work,
but the special requirements of the GNU Affero General Public License,
section 13, concerning
interaction through a network will apply to the
combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of
the GNU General Public License from time to time. Such new versions will
be similar in spirit to the present version, but may differ in detail to
address new problems or concerns.

Each version is given a distinguishing version number. If the
Program specifies that a certain numbered version of the GNU General
Public License "or any later version" applies to it, you have the
option of following the terms and conditions either of that numbered
version or of any later version published by the Free Software
Foundation. If the Program does not specify a version number of the
GNU General Public License, you may choose any version ever published
by the Free Software Foundation.

If the Program specifies that a proxy can decide which future
versions of the GNU General Public License
can be used, that proxy's
public statement of acceptance of a version permanently authorizes you
to choose that version for the Program.

Later license versions may give you additional or different
permissions. However, no additional obligations are imposed on any
author or copyright holder as a result of your choosing to follow a
later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY
APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT
HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY
OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM
IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF
ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT

UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING
WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS
THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY
GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE
USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF
DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD
PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS),
EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF
SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided
above cannot be given local legal effect according to their terms,
reviewing courts shall apply local law that most closely approximates
an absolute waiver of all civil liability in connection with the
Program, unless a warranty or assumption of liability accompanies a
copy
of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest
possible use to the public, the best way to achieve this is to make it
free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest
to attach them to the start of each source file to most effectively
state the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation, either version 3 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>
This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of
the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what you want to do, use the GNU Lesser General
Public License instead of this License. But first, please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.

GNU Free Documentation License
Version 1.3, 3 November 2008

Copyright (C) 2000, 2001, 2002, 2007, 2008 Free Software Foundation, Inc.
<http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other
functional and useful document "free" in the sense of freedom: to
assure everyone the effective freedom to copy and redistribute it,
with or without modifying it, either commercially or noncommercially.
Secondarily, this License preserves for the author and publisher a way
to get credit for their work, while not being considered responsible
for modifications made by others.

This License is a kind of "copyleft", which means that derivative

works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free
software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept
the license if you
copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated,
as being those of Invariant Sections, in the notice
that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero

Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing
editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available,
and the
machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

The "publisher" means any person or entity that distributes copies of the Document to the public.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements",

"Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent

pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through
your agents or retailers) of that
edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
D. Preserve all the copyright notices of the Document.
E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the

terms of this License, in the form shown in the Addendum below.
G. Preserve in that license notice the full lists of Invariant Sections
and required Cover Texts given in the Document's
license notice.
H. Include an unaltered copy of this License.
I. Preserve the section Entitled "History", Preserve its Title, and add
to it an item stating at least the title, year, new authors, and
publisher of the Modified Version as given on the Title Page. If
there is no section Entitled "History" in the Document, create one
stating the title, year, authors, and publisher of the Document as
given on its Title Page, then add an item describing the Modified
Version as stated in the previous sentence.
J. Preserve the network location, if any, given in the Document for
public access to a Transparent copy of the Document, and likewise
the network locations given in the Document for previous versions
it was based on. These may be placed in the "History" section.
You may omit a network location for a work that was published at
least four years before the Document itself, or if the original
publisher of the version it refers to gives
permission.
K. For any section Entitled "Acknowledgements" or "Dedications",
Preserve the Title of the section, and preserve in the section all
the substance and tone of each of the contributor acknowledgements
and/or dedications given therein.
L. Preserve all the Invariant Sections of the Document,
unaltered in their text and in their titles. Section numbers
or the equivalent are not considered part of the section titles.
M. Delete any section Entitled "Endorsements". Such a section
may not be included in the Modified Version.
N. Do not retitle any existing section to be Entitled "Endorsements"
or to conflict in title with any Invariant Section.
O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or
appendices that qualify as Secondary Sections and contain no material
copied from the Document, you may at your option designate some or all
of these sections as invariant. To do this, add their titles
to the
list of Invariant Sections in the Modified Version's license notice.
These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains
nothing but endorsements of your Modified Version by various
parties--for example, statements of peer review or that the text has
been approved by an organization as the authoritative definition of a
standard.

You may add a passage of up to five words as a Front-Cover Text, and a

passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from
the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name
of the original
author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all

other respects.

You may extract a single document from such a collection, and distribute it individually
under this License, provided you insert a
copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within
the aggregate, or the
electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If

a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation
by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a
particular numbered version of this
License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or

of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

11. RELICENSING

"Massive Multiauthor Collaboration Site" (or "MMC Site") means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A "Massive Multiauthor Collaboration" (or "MMC") contained in the site means any set of copyrightable works thus published on the MMC site.

"CC-BY-SA" means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

"Incorporate" means to publish or republish a Document, in whole or in part, as part of another Document.

An MMC is "eligible for relicensing" if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

Copyright (c) YEAR YOUR NAME.
Permission is granted to copy, distribute and/or modify this document

under the terms of the GNU Free Documentation License, Version 1.3
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled "GNU
Free Documentation License".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts,
replace the "with...Texts." line with this:

with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If
you have Invariant Sections without Cover Texts, or some other
combination of the three, merge those two alternatives to suit the
situation.

If your document contains nontrivial examples of program code, we
recommend releasing these examples in parallel under your choice of
free software license, such as the GNU General Public License,
to permit their use in free software.

1.4 xinetd 2.3.15

1.4.1 Available under license :

This software is

(c) Copyright 1992 by Panagiotis Tsirigotis

The author (Panagiotis Tsirigotis) grants permission to use, copy,
and distribute this software and its documentation for any purpose
and without fee, provided that the above copyright notice extant in
files in this distribution is not removed from files included in any
redistribution and that this copyright notice is also included in any
redistribution.

Modifications to this software may be distributed, either by distributing
the modified software or by distributing patches to the original software,
under the following additional terms:

1. The version number will be modified as follows:
   a. The first 3 components of the version number
      (i.e <number>.<number>.<number>) will remain unchanged.
   b. A new component will be appended to the version number to indicate
      the modification level. The form of this component is up to the
      author of the modifications.

2. The author
of the modifications will include his/her name by appending it
along with the new version number to this file and will be responsible for
any wrong behavior of the modified software.

The author makes no representations about the suitability of this
software for any purpose. It is provided "as is" without any express
or implied warranty.

Modifications:
Version: 2.1.8.7-current
Copyright 1998-2001 by Rob Braun
/*
* ++Copyright++ 1983, 1990, 1993
* -
* Copyright (c) 1983, 1990, 1993
*   The Regents of the University of California. All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the above copyright
*   notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*   notice, this list of conditions and the following disclaimer in the
*   documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*   must display the following acknowledgement:
*   This product includes software developed by the University of
*   California, Berkeley and its contributors.
* 4. Neither the name of the University nor the names of its contributors
*   may be used to endorse or promote products derived from this software
*   without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
* -
* Portions Copyright (c) 1993 by Digital Equipment Corporation.
*

* Permission
 to use, copy, modify, and distribute this software for any
* purpose with or without fee is hereby granted, provided that the above
* copyright notice and this permission notice appear in all copies, and that
* the name of Digital Equipment Corporation not be used in advertising or
* publicity pertaining to distribution of the document or software without
* specific, written prior permission.
*
* THE SOFTWARE IS PROVIDED "AS IS" AND DIGITAL EQUIPMENT CORP. DISCLAIMS ALL
* WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES
* OF MERCHANTABILITY AND FITNESS.   IN NO EVENT SHALL DIGITAL EQUIPMENT
* CORPORATION BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL
* DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR
* PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS
* ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS
* SOFTWARE.
* -
* --Copyright--
*/
This software is

(c) Copyright 1992, 1993 by Panagiotis Tsirigotis

The author (Panagiotis Tsirigotis) grants permission to use, copy,
and distribute this software and its documentation for any purpose
and without fee, provided that a) the above copyright notice extant in
files in this distribution is not removed from files included in any
redistribution, and b) this file is also included in any redistribution.

Modifications to this software may be distributed, either by distributing
the modified software or by distributing patches to the original software,
under the following additional terms:

1. The version number will be modified as follows:
   a. The first 3 components of the version number
      (i.e. <number>.<number>.<number>) will remain unchanged.
   b. A new component will be appended to the version number to indicate
      the modification level. The form of this component is up to the
      author of the modifications.

2. The author
 of the modifications will include his/her name by appending it
  along with the new version number to this file and will be responsible for
  any wrong behavior of the modified software.

The author makes no representations about the suitability of this
software for any purpose. It is provided "as is" without any express
or implied warranty.

/*
* Copyright (c) 1988, 1993
*	The Regents of the University of California. All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the above copyright
*   notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*   notice, this list of conditions and the following disclaimer in the
*   documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*   must display the following acknowledgement:
*	This product includes software developed by the University of
*	California, Berkeley and its contributors.
* 4. Neither the name of the University nor the names of its contributors
*   may be used to endorse or promote products
 derived from this software
*   without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*/
ORIGINAL LICENSE:
This software is

(c) Copyright 1992 by Panagiotis Tsirigotis

The author (Panagiotis Tsirigotis) grants permission to use, copy,
and distribute this software and its documentation for any purpose
and without fee, provided that the above copyright notice extant in
files in this distribution is not removed from files included in any
redistribution and that this copyright notice is also included in any
redistribution.

Modifications to this software may be distributed, either by distributing
the modified software or by distributing patches to the original software,
under the following additional terms:

1. The version number will be modified as follows:
   a. The first 3 components of the version number
      (i.e <number>.<number>.<number>) will remain unchanged.
   b. A new component will be appended to the version number to indicate
      the modification level. The form of this component is up to the
      author of the modifications.

2.
 The author of the modifications will include his/her name by appending it
 along with the new version number to this file and will be responsible for
 any wrong behavior of the modified software.

The author makes no representations about the suitability of this
software for any purpose. It is provided "as is" without any express
or implied warranty.

Modifications:
Version: 2.1.8.7-current
Copyright 1998-2001 by Rob Braun

Sensor Addition
Version: 2.1.8.9pre14a
Copyright 2001 by Steve Grubb

This is an exerpt from an email I recieved from the original author, allowing
xinetd as maintained by me, to use the higher version numbers:

I appreciate your maintaining the version string guidelines as specified
in the copyright. But I did not mean them to last as long as they did.

So, if you want, you may use any 2.N.* (N >= 3) version string for future
xinetd versions that you release. Note that I am excluding the 2.2.* line;
using
 that would only create confusion. Naming the next release 2.3.0
would put to rest the confusion about 2.2.1 and 2.1.8.*.

1.5 bzip2 1.0.6

1.5.1 Available under license :

This program, "bzip2" and associated library "libbzip2", are
copyright (C) 1996-2002 Julian R Seward. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions

are met:

1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.

2. The origin of this software must not be misrepresented; you must
not claim that you wrote the original software. If you use this
software in a product, an acknowledgment in the product
documentation would be appreciated but is not required.

3. Altered source versions must be plainly marked as such, and must
not be misrepresented as being the original software.

4. The name of the author may not be used to endorse or promote
products derived from this software without specific prior written
permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR
"AS IS" AND ANY EXPRESS
OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY
DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE
GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Julian Seward, Cambridge, UK.
jseward@acm.org
bzip2/libbzip2 version 1.0.2 of 30 December 2001

%%CreationDate: Wed Dec 22 1999
% Copyright (URW)++,Copyright 1999 by (URW)++ Design & Development
% (URW)++,Copyright 1999 by (URW)++ Design & Development
% See the file COPYING (GNU General Public License) for license conditions.
% As a special exception, permission is granted to include this font
% program in a Postscript or PDF file that consists of a document that
% contains text to be displayed or printed using this font, regardless
% of the conditions or license applying to the document itself.

/Notice ((URW)++,Copyright 1999 by (URW)++ Design & Development. See the file COPYING (GNU General Public License) for license conditions. As a special exception, permission is granted to include this font program in a Postscript or PDF file that consists of a document that contains text to be displayed or printed using this font, regardless of the conditions or license applying to the document itself.) readonly def
/Copyright (Copyright (URW)++,Copyright 1999 by (URW)++ Design

```
 & Development) readonly def
/*
  minibz2
    libbz2.dll test program.
    by Yoshioka Tsuneo (tsuneo@rr.iij4u.or.jp)
    This file is Public Domain.  Welcome any email to me.

  usage: minibz2 [-d] [-{1,2,..9}] [[srcfilename] destfilename]
*/
```

1.6 binutils 2.24

1.6.1 Available under license :

```
GNU GENERAL PUBLIC LICENSE
        Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
    51 Franklin Street, Fifth Floor, Boston, MA  02110-1301  USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

       Preamble

 The licenses for most software are designed to take away your
freedom to share and change it.  By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users.  This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it.  (Some other Free Software Foundation software is covered by
the GNU Library General Public License instead.)  You can apply it to
your programs, too.

 When we speak of free software, we are referring to freedom, not
price.  Our General Public Licenses are designed
 to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

 To protect your rights, we need to make restrictions that forbid
anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate to certain responsibilities for you if you
distribute copies of the software, or if you modify it.

 For example, if you distribute copies of such a program, whether
```

gratis or for a fee, you must give the recipients all the rights that
you have. You must make sure that they, too, receive or can get the
source code. And you must show them these terms so they know their
rights.

We protect your rights with two steps: (1) copyright the software, and
(2) offer you this license which gives you legal permission to copy,
distribute
and/or modify the software.

Also, for each author's protection and ours, we want to make certain
that everyone understands that there is no warranty for this free
software. If the software is modified by someone else and passed on, we
want its recipients to know that what they have is not the original, so
that any problems introduced by others will not reflect on the original
authors' reputations.

Finally, any free program is threatened constantly by software
patents. We wish to avoid the danger that redistributors of a free
program will individually obtain patent licenses, in effect making the
program proprietary. To prevent this, we have made it clear that any
patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and
modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which
contains
a notice placed by the copyright holder saying it may be distributed
under the terms of this General Public License. The "Program", below,
refers to any such program or work, and a "work based on the Program"
means either the Program or any derivative work under copyright law:
that is to say, a work containing the Program or a portion of it,
either verbatim or with modifications and/or translated into another
language. (Hereinafter, translation is included without limitation in
the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not
covered by this License; they are outside its scope. The act of
running the Program is not restricted, and the output from the Program
is covered only if its contents constitute a work based on the
Program (independent of having been made by running the Program).
Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies

of the Program's
source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole
or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered
independent and separate works in
themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest

your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the

source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each
time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution
of the Program by
all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any

patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through
any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number
of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW.

EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN
IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License

along with this program; if not, write to the Free Software
Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show
w' and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this is what you want to do, use the GNU Library General
Public License instead of this License.
GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts
as the successor of the GNU Library Public License, version 2, hence
the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest
you first think carefully about whether
this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients
all the rights that we gave
you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence

of
any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits
its criteria of freedom. The Lesser General
Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use
the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the

users' freedom, it does ensure that the user of a program that is
linked with the Library has the freedom and the wherewithal to run
that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and
modification follow. Pay close attention to the difference between a
"work based on the library" and a "work that uses the library". The
former contains code derived from the library, whereas the latter must
be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other
program which contains a notice placed by the copyright holder or
other authorized party saying it may be distributed under the terms of
this Lesser General Public License (also called "this License").
Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data
prepared so as to be conveniently linked with application programs
(which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work
which has been distributed under these terms. A "work based on the
Library" means either the Library or any derivative work under
copyright law: that is to say, a work containing the Library or a
portion of it, either verbatim or with modifications and/or translated
straightforwardly into another language. (Hereinafter, translation is
included without
limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for
making modifications to it. For a library, complete source code means
all the source code for all modules it contains, plus any associated
interface definition files, plus the scripts used to control compilation
and installation of the library.

Activities other than copying, distribution and modification are not
covered by this License; they are outside its scope. The act of
running a program using the Library is not restricted, and output from
such a program is covered only if its contents constitute a work based
on the Library (independent of the use of the Library in a tool for
writing it). Whether that is true depends on what the Library does
and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's
complete source code as you receive it, in any medium, provided that

you conspicuously and appropriately publish
on each copy an
appropriate copyright notice and disclaimer of warranty; keep intact
all the notices that refer to this License and to the absence of any
warranty; and distribute a copy of this License along with the
Library.

You may charge a fee for the physical act of transferring a copy,
and you may at your option offer warranty protection in exchange for a
fee.

2. You may modify your copy or copies of the Library or any portion
of it, thus forming a work based on the Library, and copy and
distribute such modifications or work under the terms of Section 1
above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices
stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no
charge to all third parties under the terms of this License.

d) If a facility in the modified
Library refers to a function or a
table of data to be supplied by an application program that uses
the facility, other than as an argument passed when the facility
is invoked, then you must make a good faith effort to ensure that,
in the event an application does not supply such function or
table, the facility still operates, and performs whatever part of
its purpose remains meaningful.

(For example, a function in a library to compute square roots has
a purpose that is entirely well-defined independent of the
application. Therefore, Subsection 2d requires that any
application-supplied function or table used by this function must
be optional: if the application does not supply it, the square
root function must still compute square roots.)

These requirements apply to the modified work as a whole. If
identifiable sections of that work are not derived from the Library,
and can be reasonably considered independent and separate works in
themselves,
then this License, and its terms, do not apply to those
sections when you distribute them as separate works. But when you
distribute the same sections as part of a whole which is a work based
on the Library, the distribution of the whole must be on the terms of

this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a

work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License.
Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables
containing that work also fall under Section 6,
whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable

source code for the Library including whatever
changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user
installs one, as long as the modified version is
interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major
components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot

distribute
so as to satisfy simultaneously your obligations under this
License and any other pertinent obligations, then as a consequence you
may not distribute the Library at all. For example, if a patent
license would not permit royalty-free redistribution of the Library by
all those who receive copies directly or indirectly through you, then
the only way you could satisfy both it and this License would be to
refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any
particular circumstance, the balance of the section is intended to apply,
and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any
patents or other property right claims or to contest validity of any
such claims; this section has the sole purpose of protecting the
integrity of the free software distribution system which is
implemented by public license practices. Many people
have made
generous contributions to the wide range of software distributed
through that system in reliance on consistent application of that
system; it is up to the author/donor to decide if he or she is willing
to distribute software through any other system and a licensee cannot
impose that choice.

This section is intended to make thoroughly clear what is believed to
be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in
certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Library under this License may add
an explicit geographical distribution limitation excluding those countries,
so that distribution is permitted only in or among countries not thus
excluded. In such case, this License incorporates the limitation as if
written in the body of this License.

13. The Free Software Foundation may publish revised and/or new
versions of the Lesser General Public
License from time to time.
Such new versions will be similar in spirit to the present version,
but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library
specifies a version number of this License which applies to it and
"any later version", you have the option of following the terms and
conditions either of that version or of any later version published by
the Free Software Foundation. If the Library does not specify a
license version number, you may choose any version ever published by

the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of
all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL
DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively

convey the exclusion of warranty; and each file should have at least the
"copyright" line
and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or
modify it under the terms of the GNU Lesser General Public
License as published by the Free Software Foundation; either
version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public
License along with this library; if not, write to the Free Software
Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should
also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the library, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the
library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!
GNU LESSER GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates
the terms and conditions of version 3 of the GNU General Public
License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and the "GNU GPL" refers to version 3 of the GNU General Public License.

"The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An "Application" is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of
this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from
a header file that is part of the Library. You may convey such object
code under terms of your choice, provided that, if the incorporated
material is not limited to numerical parameters, data structure
layouts
and accessors, or small macros, inline functions and templates
(ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the
Library is used in it and that the Library and its use are
covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license
document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that,
taken together, effectively do not restrict modification of the
portions of the Library contained in the Combined Work and reverse
engineering for debugging such modifications, if you also do each of
the following:

a) Give prominent notice with each copy of the Combined Work that
the Library is used in it and that the Library and its use are
covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license
document.

c) For a Combined Work that displays copyright
notices during
execution, include the copyright notice for the Library among
these notices, as well as a reference directing the user to the
copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this
License, and the Corresponding Application Code in a form
suitable for, and under terms that permit, the user to
recombine or relink the Application with a modified version of
the Linked Version to produce a modified Combined Work, in the

manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the

Library as you received it specifies that a certain numbered version
of the GNU Lesser General Public License "or any later version"
applies to it, you have the option of following the
terms and
conditions either of that published version or of any later version
published by the Free Software Foundation. If the Library as you
received it does not specify a version number of the GNU Lesser
General Public License, you may choose any version of the GNU Lesser
General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide
whether future versions of the GNU Lesser General Public License shall
apply, that proxy's public statement of acceptance of any version is
permanent authorization for you to choose that version for the
Library.

GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for
software and other kinds of works.

The licenses for most software and other practical works are designed
to take away your freedom to share and change the works. By contrast,
the GNU General Public License is intended to guarantee your freedom to
share and change all versions of a program--to make sure it remains free
software for all its users. We, the Free Software Foundation, use the
GNU General Public License for most of our software; it applies also to
any other work released this way by its authors. You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price.

Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
them if you wish), that you receive source code or can get it if you
want it, that you can change the software or use pieces of it in new
free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you
these rights or asking you to surrender the rights. Therefore, you have
certain responsibilities if you distribute copies of the software, or if
you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may
be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of

an executable work include anything, other
than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs
which are used unmodified in performing those activities but
which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License
only if the output, given its
content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with

the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes
it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each
copy an appropriate copyright notice;
keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified

it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as

long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product

is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately

under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply
either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you
cure the violation prior to 30 days after
your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do

not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free

patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly
available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent
license
you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement,

or that patent
license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding
any other provision of this License, you have
permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the
option of
following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF
ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of
Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest
possible use to the public, the best way to achieve this is to make it
free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest
to attach them to the start of each source file to most effectively
state the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation, either version 3 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

<program> Copyright
(C) <year> <name of author>
This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with

the library. If this is what you want to do, use the GNU Lesser General
Public License instead of this License. But first, please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.
GNU LIBRARY GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the library GPL. It is
numbered 2 because it goes with version 2 of the ordinary GPL.]

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
Licenses are intended to guarantee your freedom to share and change
free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some
specially designated Free Software Foundation software, and to any
other libraries whose authors decide to use it. You can use it for
your libraries, too.

When we speak of free software, we are referring to freedom, not
price. Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid
anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate to certain responsibilities for you if
you distribute copies of the library, or if you modify it.

For example, if you distribute copies of the library, whether gratis
or for a fee, you must give the recipients all the rights that we gave
you. You must make sure that they, too, receive or can get the source
code. If you link a program with the library, you must provide
complete object files to the recipients so that they can relink them
with the library, after making changes to the library and recompiling
it. And you must show them these terms so they know their rights.

Our method of protecting your rights has two steps: (1) copyright the library, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the library.

Also, for each distributor's protection, we want to make certain that everyone understands that there is no warranty for this free library. If the library is modified by someone else and passed on, we want its recipients to know that what they have is not the original version, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that companies distributing free software will individually obtain patent licenses, thus in effect transforming the program into proprietary software. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License, which was designed for utility programs. This license, the GNU Library General Public License, applies to certain designated libraries. This license is quite different from the ordinary one; be sure to read it in full, and don't assume that anything in it is the same as in the ordinary license.

The reason we have a separate public license for some libraries is that they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and legal sense, the linked executable is a combined work, a derivative of the original library, and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public License for libraries did not effectively promote software sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve

this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

GNU LIBRARY GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of

the use of the Library in a tool for
writing it). Whether that is true depends on what the Library does
and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's
complete source code as you receive it, in any medium, provided that
you conspicuously and appropriately publish on each copy an
appropriate copyright notice and disclaimer of warranty; keep intact
all the notices that refer to this License and to the absence of any
warranty; and distribute a copy of this License along with the
Library.

You may charge a fee for the physical act of transferring a copy,
and you may at your option offer warranty protection in exchange for a
fee.

2. You may modify your copy or copies of the Library or any portion
of it, thus forming a work based on the Library, and copy and
distribute such modifications or work under the terms of Section 1
above, provided that you also meet all of these conditions:

a) The modified work must itself
be a software library.

b) You must cause the files modified to carry prominent notices
stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no
charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a
table of data to be supplied by an application program that uses
the facility, other than as an argument passed when the facility
is invoked, then you must make a good faith effort to ensure that,
in the event an application does not supply such function or
table, the facility still operates, and performs whatever part of
its purpose remains meaningful.

(For example, a function in a library to compute square roots has
a purpose that is entirely well-defined independent of the
application. Therefore, Subsection 2d requires that any
application-supplied function or table used by this function
must
be optional: if the application does not supply it, the square
root function must still compute square roots.)

These requirements apply to the modified work as a whole. If
identifiable sections of that work are not derived from the Library,

and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition,
mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the
Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not

compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also compile or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference

directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

c) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

d) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise

permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by

all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Library General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is

copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Appendix: How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year>

<name of author>

This library is free software; you can redistribute it and/or
modify it under the terms of the GNU Library General Public
License as published by the Free Software Foundation; either
version 2 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
Library General Public License for more details.

You should have received a copy of the GNU Library General Public
License along with this library; if not, write to the Free
Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston,
MA 02110-1301, USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the library, if
necessary. Here
is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the
library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

1.7 python 3.5.1

1.7.1 Available under license :

Copyright (c) 2002 Jorge Acereda <jacereda@users.sourceforge.net> &
Peter O'Gorman <ogorman@users.sourceforge.net>

Portions may be copyright others, see the AUTHORS file included with this
distribution.

Maintained by Peter O'Gorman <ogorman@users.sourceforge.net>

Bug Reports and other queries should go to <ogorman@users.sourceforge.net>

Permission is hereby granted, free of charge, to any person obtaining

a copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY
KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE
LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION
WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
libffi - Copyright (c) 1996-2003 Red Hat, Inc.

Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
``Software''), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be included
in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED ``AS IS'', WITHOUT WARRANTY OF ANY KIND, EXPRESS
OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.
IN NO EVENT SHALL CYGNUS SOLUTIONS BE LIABLE FOR ANY CLAIM, DAMAGES OR
OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE,
ARISING FROM, OUT OF OR IN CONNECTION WITH
THE SOFTWARE OR THE USE OR
OTHER DEALINGS IN THE SOFTWARE.
X Window System License - X11R6.4

Copyright (c) 1998 The Open Group

Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to

permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.
IN NO EVENT SHALL THE OPEN GROUP BE LIABLE FOR ANY CLAIM, DAMAGES OR
OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE,
ARISING FROM, OUT OF OR IN CONNECTION
WITH THE SOFTWARE OR THE USE OR
OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of The Open Group shall
not be used in advertising or otherwise to promote the sale, use or
other dealings in this Software without prior written authorization
from The Open Group.

X Window System is a trademark of The Open Group
A. HISTORY OF THE SOFTWARE
==========

Python was created in the early 1990s by Guido van Rossum at Stichting
Mathematisch Centrum (CWI, see http://www.cwi.nl) in the Netherlands
as a successor of a language called ABC. Guido remains Python's
principal author, although it includes many contributions from others.

In 1995, Guido continued his work on Python at the Corporation for
National Research Initiatives (CNRI, see http://www.cnri.reston.va.us)
in Reston, Virginia where he released several versions of the
software.

In May 2000, Guido and the Python core development team moved to
BeOpen.com to form the BeOpen PythonLabs team. In October of the same
year, the PythonLabs team moved to Digital Creations (now Zope
Corporation, see http://www.zope.com). In 2001, the Python Software
Foundation (PSF, see http://www.python.org/psf/) was formed, a
non-profit organization created specifically to own Python-related
Intellectual Property. Zope Corporation is a sponsoring member
of
the PSF.

All Python releases are Open Source (see http://www.opensource.org for
the Open Source Definition). Historically, most, but not all, Python
releases have also been GPL-compatible; the table below summarizes
the various releases.

Release	Derived from	Year	Owner	GPL-compatible? (1)
0.9.0 thru 1.2		1991-1995	CWI	yes
1.3 thru 1.5.2	1.2	1995-1999	CNRI	yes
1.6	1.5.2	2000	CNRI	no
2.0	1.6	2000	BeOpen.com	no
1.6.1	1.6	2001	CNRI	yes (2)
2.1	2.0+1.6.1	2001	PSF	no
2.0.1	2.0+1.6.1	2001	PSF	yes
2.1.1	2.1+2.0.1	2001	PSF	yes
2.1.2	2.1.1	2002	PSF	yes
2.1.3	2.1.2	2002	PSF	yes
2.2 and above				
2.1.1		2001-now	PSF	yes

Footnotes:

(1) GPL-compatible doesn't mean that we're distributing Python under the GPL. All Python licenses, unlike the GPL, let you distribute a modified version without making your changes open source. The GPL-compatible licenses make it possible to combine Python with other software that is released under the GPL; the others don't.

(2) According to Richard Stallman, 1.6.1 is not GPL-compatible, because its license has a choice of law clause. According to CNRI, however, Stallman's lawyer has told CNRI's lawyer that 1.6.1 is "not incompatible" with the GPL.

Thanks to the many outside volunteers who have worked under Guido's direction to make these releases possible.

B. TERMS AND CONDITIONS FOR ACCESSING OR OTHERWISE USING PYTHON
==========

PYTHON SOFTWARE FOUNDATION LICENSE VERSION 2
---

1. This LICENSE AGREEMENT
is between the Python Software Foundation
("PSF"), and the Individual or Organization ("Licensee") accessing and
otherwise using this software ("Python") in source or binary form and
its associated documentation.

2. Subject to the terms and conditions of this License Agreement, PSF hereby
grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce,

analyze, test, perform and/or display publicly, prepare derivative works,
distribute, and otherwise use Python alone or in any derivative version,
provided, however, that PSF's License Agreement and PSF's notice of copyright,
i.e., "Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010,
2011, 2012, 2013, 2014, 2015 Python Software Foundation; All Rights Reserved"
are retained in Python alone or in any derivative version prepared by Licensee.

3. In the event Licensee prepares a derivative work that is based on
or incorporates Python or any part thereof, and wants to make
the derivative work available
to others as provided herein, then
Licensee hereby agrees to include in any such work a brief summary of
the changes made to Python.

4. PSF is making Python available to Licensee on an "AS IS"
basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR
IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND
DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS
FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON WILL NOT
INFRINGE ANY THIRD PARTY RIGHTS.

5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON
FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS
A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON,
OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

6. This License Agreement will automatically terminate upon a material
breach of its terms and conditions.

7. Nothing in this License Agreement shall be deemed to create any
relationship of agency, partnership, or joint venture between PSF
and
Licensee. This License Agreement does not grant permission to use PSF
trademarks or trade name in a trademark sense to endorse or promote
products or services of Licensee, or any third party.

8. By copying, installing or otherwise using Python, Licensee
agrees to be bound by the terms and conditions of this License
Agreement.

BEOPEN.COM LICENSE AGREEMENT FOR PYTHON 2.0

BEOPEN PYTHON OPEN SOURCE LICENSE AGREEMENT VERSION 1

1. This LICENSE AGREEMENT is between BeOpen.com ("BeOpen"), having an
office at 160 Saratoga Avenue, Santa Clara, CA 95051, and the

Individual or Organization ("Licensee") accessing and otherwise using
this software in source or binary form and its associated
documentation ("the Software").

2. Subject to the terms and conditions of this BeOpen Python License
Agreement, BeOpen hereby grants Licensee a non-exclusive,
royalty-free, world-wide license to reproduce, analyze, test, perform
and/or display publicly, prepare
derivative works, distribute, and
otherwise use the Software alone or in any derivative version,
provided, however, that the BeOpen Python License is retained in the
Software, alone or in any derivative version prepared by Licensee.

3. BeOpen is making the Software available to Licensee on an "AS IS"
basis. BEOPEN MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR
IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, BEOPEN MAKES NO AND
DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS
FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE SOFTWARE WILL NOT
INFRINGE ANY THIRD PARTY RIGHTS.

4. BEOPEN SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF THE
SOFTWARE FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS
AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THE SOFTWARE, OR ANY
DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

5. This License Agreement will automatically terminate upon a material
breach of its terms and conditions.

6. This
License Agreement shall be governed by and interpreted in all
respects by the law of the State of California, excluding conflict of
law provisions. Nothing in this License Agreement shall be deemed to
create any relationship of agency, partnership, or joint venture
between BeOpen and Licensee. This License Agreement does not grant
permission to use BeOpen trademarks or trade names in a trademark
sense to endorse or promote products or services of Licensee, or any
third party. As an exception, the "BeOpen Python" logos available at
http://www.pythonlabs.com/logos.html may be used according to the
permissions granted on that web page.

7. By copying, installing or otherwise using the software, Licensee
agrees to be bound by the terms and conditions of this License
Agreement.

CNRI LICENSE AGREEMENT FOR PYTHON 1.6.1
---

1. This LICENSE AGREEMENT is between the Corporation for National Research Initiatives, having an office at 1895 Preston White Drive, Reston, VA 20191 ("CNRI"), and the Individual or Organization ("Licensee") accessing and otherwise using Python 1.6.1 software in source or binary form and its associated documentation.

2. Subject to the terms and conditions of this License Agreement, CNRI hereby grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python 1.6.1 alone or in any derivative version, provided, however, that CNRI's License Agreement and CNRI's notice of copyright, i.e., "Copyright (c) 1995-2001 Corporation for National Research Initiatives; All Rights Reserved" are retained in Python 1.6.1 alone or in any derivative version prepared by Licensee. Alternately, in lieu of CNRI's License Agreement, Licensee may substitute the following text (omitting the quotes): "Python 1.6.1 is made available subject to the terms and conditions in CNRI's License Agreement. This Agreement together with Python 1.6.1 may be located on the Internet using the following unique, persistent identifier (known as a handle): 1895.22/1013. This Agreement may also be obtained from a proxy server on the Internet using the following URL: http://hdl.handle.net/1895.22/1013".

3. In the event Licensee prepares a derivative work that is based on or incorporates Python 1.6.1 or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python 1.6.1.

4. CNRI is making Python 1.6.1 available to Licensee on an "AS IS" basis. CNRI MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, CNRI MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON 1.6.1 WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

5. CNRI SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON 1.6.1 FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON 1.6.1, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.

7. This License Agreement shall be governed by the federal

intellectual property law of the United States, including without limitation the federal copyright law, and, to the extent such U.S. federal law does not apply, by the law of the Commonwealth of Virginia, excluding Virginia's conflict of law provisions. Notwithstanding the foregoing, with regard to derivative works based on Python 1.6.1 that incorporate non-separable material that was previously distributed under the GNU General Public License (GPL), the law of the Commonwealth of Virginia shall govern this License Agreement only as to issues arising under or with respect to Paragraphs 4,
5, and 7 of this License Agreement. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between CNRI and Licensee. This License Agreement does not grant permission to use CNRI trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.

8. By clicking on the "ACCEPT" button where indicated, or by copying, installing or otherwise using Python 1.6.1, Licensee agrees to be bound by the terms and conditions of this License Agreement.

ACCEPT

CWI LICENSE AGREEMENT FOR PYTHON 0.9.0 THROUGH 1.2

Copyright (c) 1991 - 1995, Stichting Mathematisch Centrum Amsterdam, The Netherlands. All rights reserved.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both
that copyright notice and this permission notice appear in supporting documentation, and that the name of Stichting Mathematisch Centrum or CWI not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

STICHTING MATHEMATISCH CENTRUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL STICHTING MATHEMATISCH CENTRUM BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Additional Conditions for this Windows binary build

This program is linked with and uses Microsoft Distributable Code,
copyrighted by Microsoft Corporation. The Microsoft Distributable Code
is embedded in each .exe, .dll and .pyd file as a result of running
the code through a linker.

If you further distribute programs that include the Microsoft
Distributable Code, you must comply with the restrictions on
distribution specified by Microsoft. In particular, you must require
distributors and external end users to agree to terms that protect the
Microsoft Distributable Code at least as much as Microsoft's own
requirements for the Distributable Code. See Microsoft's documentation
(included in its developer tools and on its website at microsoft.com)
for specific details.

Redistribution of the Windows binary build of the Python interpreter
complies with this agreement, provided that you do not:

- alter any copyright, trademark or patent
 notice in Microsoft's
Distributable Code;

- use Microsoft's trademarks in your programs' names or in a way that
suggests your programs come from or are endorsed by Microsoft;

- distribute Microsoft's Distributable Code to run on a platform other
than Microsoft operating systems, run-time technologies or application
platforms; or

- include Microsoft Distributable Code in malicious, deceptive or
unlawful programs.

These restrictions apply only to the Microsoft Distributable Code as
defined above, not to Python itself or any programs running on the
Python interpreter. The redistribution of the Python interpreter and
libraries is governed by the Python Software License included with this
file, or by other licenses as marked.
Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd
 and Clark Cooper
Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006 Expat maintainers.

Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including

without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be included
in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.
IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE
LIABLE FOR ANY
CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT,
TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
pybench License

This copyright notice and license applies to all files in the pybench
directory of the pybench distribution.

Copyright (c), 1997-2006, Marc-Andre Lemburg (mal@lemburg.com)
Copyright (c), 2000-2006, eGenix.com Software GmbH (info@egenix.com)

All Rights Reserved.

Permission to use, copy, modify, and distribute this software and its
documentation for any purpose and without fee or royalty is hereby
granted, provided that the above copyright notice appear in all copies
and that both that copyright notice and this permission notice appear
in supporting documentation or portions thereof, including
modifications, that you make.

THE AUTHOR MARC-ANDRE LEMBURG DISCLAIMS ALL WARRANTIES WITH REGARD TO
THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND
FITNESS, IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL,
INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING
FROM LOSS OF USE, DATA OR PROFITS, WHETHER
IN AN ACTION OF CONTRACT,
NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION
WITH THE USE OR PERFORMANCE OF THIS SOFTWARE !
libffi - Copyright (c) 1996-2014 Anthony Green, Red Hat, Inc and others.
See source files for details.

Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
``Software''), to deal in the Software without restriction, including

without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED ``AS IS'', WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.
IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY
CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF
CONTRACT,
TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
This license applies to the bootstrapper application that is embedded within the installer. It has no impact on the licensing for the rest of the installer or Python itself, as no code covered by this license exists in any other part of the product.

Microsoft Reciprocal License (MS-RL)

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions
The terms "reproduce," "reproduction," "derivative works," and "distribution" have the same meaning here as under U.S. copyright law.
A "contribution" is the original software, or any additions or changes to the software.
A "contributor" is any person that distributes its contribution under this license.
"Licensed patents" are a contributor's patent claims that read directly on its contribution.

2. Grant of Rights
(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.
(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations
(A) Reciprocal Grants- For any file you distribute that contains code from the software (in source code or binary format), you must provide recipients the source code to that file along with a copy of this license, which license will govern that file. You may license other files that are entirely your own work and

do not contain code from the software under any terms you choose.
(B) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.
(C) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.
(D) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.
(E) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.
(F) The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees or conditions.
You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

1.8 dbus-glib 0.106

1.8.1 Available under license :

The D-Bus glib bindings are licensed to you under your choice of the Academic
Free License version 2.1, or the GNU General Public License version 2. Both
licenses are included here. Some of the standalone binaries are under the GPL
only; in particular, but not limted to, tests/decode-gcov.c. Each source code
file is marked with the proper copyright information.

The Academic Free License
v. 2.1

This Academic Free License (the "License") applies to any original work of authorship (the "Original Work") whose owner (the "Licensor") has placed the following notice immediately following the copyright notice for the Original Work:

Licensed under the Academic Free License version 2.1

1) Grant of Copyright License. Licensor hereby grants You a
world-wide, royalty-free, non-exclusive, perpetual, sublicenseable
license to do the following:

a) to reproduce the Original Work in copies;

b) to prepare derivative works ("Derivative Works") based upon the Original Work;

c) to distribute copies
of the Original Work and Derivative Works to the public;

d) to perform the Original Work publicly; and

e) to display the Original Work publicly.

2) Grant of Patent License. Licensor hereby grants You a world-wide, royalty-free, non-exclusive, perpetual, sublicenseable license, under patent claims owned or controlled by the Licensor that are embodied in the Original Work as furnished by the Licensor, to make, use, sell and offer for sale the Original Work and Derivative Works.

3) Grant of Source Code License. The term "Source Code" means the preferred form of the Original Work for making modifications to it and all available documentation describing how to modify the Original Work. Licensor hereby agrees to provide a machine-readable copy of the Source Code of the Original Work along with each copy of the Original Work that Licensor distributes. Licensor reserves the right to satisfy this obligation by placing a machine-readable copy of the Source Code in an information repository
reasonably calculated to permit
inexpensive and convenient access by You for as long as Licensor continues to distribute the Original Work, and by publishing the address of that information repository in a notice immediately following the copyright notice that applies to the Original Work.

4) Exclusions From License Grant. Neither the names of Licensor, nor the names of any contributors to the Original Work, nor any of their trademarks or service marks, may be used to endorse or promote products derived from this Original Work without express prior written permission of the Licensor. Nothing in this License shall be deemed to grant any rights to trademarks, copyrights, patents, trade secrets or any other intellectual property of Licensor except as expressly stated herein. No patent license is granted to make, use, sell or offer to sell embodiments of any patent claims other than the licensed claims defined in Section 2. No right is granted to the trademarks of Licensor even if such marks
are included in the Original Work. Nothing
in this License shall be interpreted to prohibit Licensor from licensing under different terms from this License any Original Work that Licensor otherwise would have a right to license.

5) This section intentionally omitted.

6) Attribution Rights. You must retain, in the Source Code of any Derivative Works that You create, all copyright, patent or trademark notices from the Source Code of the Original Work, as well as any notices of licensing and any descriptive text identified therein as an "Attribution Notice." You must cause the Source Code for any Derivative Works that You create to carry a prominent Attribution

Notice reasonably calculated to inform recipients that You have modified the Original Work.

7) Warranty of Provenance and Disclaimer of Warranty. Licensor warrants that the copyright in and to the Original Work and the patent rights granted herein by Licensor are owned by the Licensor or are sublicensed to You under the terms of this License with the permission of the contributor(s) of those copyrights and patent rights. Except as expressly stated in the immediately proceeding sentence, the Original Work is provided under this License on an "AS IS" BASIS and WITHOUT WARRANTY, either express or implied, including, without limitation, the warranties of NON-INFRINGEMENT, MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY OF THE ORIGINAL WORK IS WITH YOU. This DISCLAIMER OF WARRANTY constitutes an essential part of this License. No license to Original Work is granted hereunder except under this disclaimer.

8) Limitation of Liability. Under no circumstances and under no legal theory, whether in tort (including negligence), contract, or otherwise, shall the Licensor be liable to any person for any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or the use of the Original Work including, without limitation, damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses. This limitation of liability shall not apply to liability for death or personal injury resulting from Licensor's negligence to the extent applicable law prohibits such limitation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this exclusion and limitation may not apply to You.

9) Acceptance and Termination. If You distribute copies of the Original Work or a Derivative Work, You must make a reasonable effort under the circumstances to obtain the express assent of recipients to the terms of this License. Nothing else but this License (or another written agreement between Licensor and You) grants You permission to create Derivative Works based upon the Original Work or to exercise any of the rights granted in Section 1 herein, and any attempt to do so except under the terms of this License (or another written agreement between Licensor and You) is expressly prohibited by U.S. copyright law, the equivalent laws of other countries, and by international treaty. Therefore, by exercising any of the rights granted to You in Section 1 herein, You indicate Your acceptance of this License and all of its terms and conditions.

10) Termination for Patent Action. This License shall terminate automatically and You may no longer exercise any of the rights granted to You by this License as of the date You commence an action, including a cross-claim or counterclaim, against Licensor or any licensee alleging that the Original Work infringes a patent. This termination provision shall not apply for an action alleging patent infringement by combinations of the Original Work with other software or hardware.

11) Jurisdiction, Venue and Governing Law. Any action or suit relating to this License may be brought only in the courts of a jurisdiction wherein the Licensor resides or in which Licensor conducts its primary
business, and under the laws of that jurisdiction excluding its conflict-of-law provisions. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any use of the Original Work outside the scope of this License or after its termination shall be subject to the requirements and penalties of the U.S. Copyright Act, 17 U.S.C. 101 et seq., the equivalent laws of other countries, and international treaty. This section shall survive the termination of this License.

12) Attorneys Fees. In any action to enforce the terms of this License or seeking damages relating thereto, the prevailing party shall be entitled to recover its costs and expenses, including, without limitation, reasonable attorneys' fees and costs incurred in connection with such action, including any appeal of such action. This section shall survive the termination of this License.

13) Miscellaneous. This License represents the complete agreement concerning
the subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable.

14) Definition of "You" in This License. "You" throughout this License, whether in upper or lower case, means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License. For legal entities, "You" includes any entity that controls, is controlled by, or is under common control with you. For purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

15) Right to Use. You may use the Original Work in all ways not otherwise restricted or conditioned by this License or by law, and

Licensor promises not to interfere with or be responsible
for such
uses by You.

This license is Copyright (C) 2003-2004 Lawrence E. Rosen. All rights
reserved. Permission is hereby granted to copy and distribute this
license without modification. This license may not be modified without
the express written permission of its copyright owner.

--
END OF ACADEMIC FREE LICENSE. The following is intended to describe the essential
differences between the Academic Free License (AFL) version 1.0 and other
open source licenses:

The Academic Free License is similar to the BSD, MIT, UoI/NCSA and Apache
licenses in many respects but it is intended to solve a few problems with
those licenses.

* The AFL is written so as to make it clear what software is being
licensed (by the inclusion of a statement following the copyright notice
in the software). This way, the license functions better than a template
license. The BSD, MIT and UoI/NCSA licenses apply to unidentified software.

* The AFL contains a complete copyright grant to the software.
The BSD
and Apache licenses are vague and incomplete in that respect.

* The AFL contains a complete patent grant to the software. The BSD, MIT,
UoI/NCSA and Apache licenses rely on an implied patent license and contain
no explicit patent grant.

* The AFL makes it clear that no trademark rights are granted to the
licensor's trademarks. The Apache license contains such a provision, but the
BSD, MIT and UoI/NCSA licenses do not.

* The AFL includes the warranty by the licensor that it either owns the
copyright or that it is distributing the software under a license. None of
the other licenses contain that warranty. All other warranties are disclaimed,
as is the case for the other licenses.

* The AFL is itself copyrighted (with the right granted to copy and distribute
without modification). This ensures that the owner of the copyright to the
license will control changes. The Apache license contains a copyright notice,
but the BSD, MIT and UoI/NCSA licenses do
not.
--
START OF GNU GENERAL PUBLIC LICENSE

--

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not
price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license
which gives you legal permission to copy,
distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain

that everyone understands that there is no warranty for this free
software. If the software is modified by someone else and passed on, we
want its recipients to know that what they have is not the original, so
that any problems introduced by others will not reflect on the original
authors' reputations.

Finally, any free program is threatened constantly by software
patents. We wish to avoid the danger that redistributors of a free
program will individually obtain patent licenses, in effect making the
program proprietary. To prevent this, we have made it clear that any
patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and
modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0.
This License applies to any program or other work which contains
a notice placed by the copyright holder saying it may be distributed
under the terms of this General Public License. The "Program", below,
refers to any such program or work, and a "work based on the Program"
means either the Program or any derivative work under copyright law:
that is to say, a work containing the Program or a portion of it,
either verbatim or with modifications and/or translated into another
language. (Hereinafter, translation is included without limitation in
the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not
covered by this License; they are outside its scope. The act of
running the Program is not restricted, and the output from the Program
is covered only if its contents constitute a work based on the
Program (independent of having been made by running the Program).
Whether that is true depends on what the Program
does.

1. You may copy and distribute verbatim copies of the Program's
source code as you receive it, in any medium, provided that you
conspicuously and appropriately publish on each copy an appropriate
copyright notice and disclaimer of warranty; keep intact all the
notices that refer to this License and to the absence of any warranty;
and give any other recipients of the Program a copy of this License
along with the Program.

You may charge a fee for the physical act of transferring a copy, and
you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You

may copy and distribute the Program (or a work based on it,
under Section 2) in object code or executable form under the terms of
Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable
source code, which must be distributed under the terms of Sections
1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three
years, to give any third party, for a charge no more than your
cost of physically performing source distribution, a complete
machine-readable copy of the corresponding source code, to be
distributed under the terms of Sections 1 and 2 above on a medium
customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer
to distribute corresponding source code. (This alternative is
allowed only for noncommercial distribution and only
if you
received the program in object code or executable form with such
an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for
making modifications to it. For an executable work, complete source
code means all the source code for all modules it contains, plus any
associated interface definition files, plus the scripts used to
control compilation and installation of the executable. However, as a
special exception, the source code distributed need not include
anything that is normally distributed (in either source or binary
form) with the major components (compiler, kernel, and so on) of the
operating system on which the executable runs, unless that component
itself accompanies the executable.

If distribution of executable or object code is made by offering
access to copy from a designated place, then offering equivalent
access to copy the source code from the same place counts as
distribution of the source code,
even though third parties are not
compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program
except as expressly provided under this License. Any attempt
otherwise to copy, modify, sublicense or distribute the Program is
void, and will automatically terminate your rights under this License.
However, parties who have received copies, or rights, from you under
this License will not have their licenses terminated so long as such
parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the
Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example,
if a patent
license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide
if he or she is willing
to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to
be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in
certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Program under this License
may add an explicit geographical distribution limitation excluding
those countries, so that distribution is permitted only in or among
countries not thus excluded. In such case, this License incorporates
the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions
of the General Public License from time to time. Such new versions will
be similar in spirit to the present version, but may differ in detail to
address new problems or concerns.

Each version is given a distinguishing version
number. If the Program
specifies a version number of this License which applies to it and "any
later version", you have the option of following the terms and conditions
either of that version or of any later version published by the Free
Software Foundation. If the Program does not specify a version number of
this License, you may choose any version ever published by the Free Software
Foundation.

10. If you wish to incorporate parts of the Program into other free
programs whose distribution conditions are different, write to the author
to ask for permission. For software which is copyrighted by the Free
Software Foundation, write to the Free Software Foundation; we sometimes
make exceptions for this. Our decision will be guided by the two goals
of preserving the free status of all derivatives of our free software and
of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY
FOR THE
PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES
PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED
OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS
TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE
PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING,
REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING

WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF
THE PROGRAM TO OPERATE WITH ANY OTHER
PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free
Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show
c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General
Public
License instead of this License.

1.9 findutils 4.6.0

1.9.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free

software for all its users. We, the Free Software Foundation, use the
GNU General Public License for most of our software; it applies also to
any other work released this way by its authors. You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price. Our General Public Licenses
are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
them if you wish), that you receive source code or can get it if you
want it, that you can change the software or use pieces of it in new
free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you
these rights or asking you to surrender the rights. Therefore, you have
certain responsibilities if you distribute copies of the software, or if
you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether
gratis or for a fee, you must pass on to the recipients the same
freedoms that you received. You must make sure that they, too, receive
or can get the source code. And you must show them these terms so they
know their rights.

Developers that use the GNU GPL protect your rights with two steps:
(1) assert copyright on the software, and (2) offer
you this License
giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains
that there is no warranty for this free software. For both users' and
authors' sake, the GPL requires that modified versions be marked as
changed, so that their problems will not be attributed erroneously to
authors of previous versions.

Some devices are designed to deny users access to install or run
modified versions of the software inside them, although the manufacturer
can do so. This is fundamentally incompatible with the aim of
protecting users' freedom to change the software. The systematic
pattern of such abuse occurs in the area of products for individuals to
use, which is precisely where it is most unacceptable. Therefore, we
have designed this version of the GPL to prohibit the practice for those
products. If such problems arise substantially in other domains, we
stand ready to extend this provision to those domains
in future versions
of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents.

States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To
"modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate
Legal Notices"
to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the

work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than
the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing
those activities but
which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content,
constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users'
Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice;

keep
intact all notices stating that this License and any
non-permissive terms added in accord with section 7 apply to the code;
keep intact all notices of the absence of any warranty; and give all
recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey,
and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to
produce it from the Program, in the form of source code under the
terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified
it, and giving a relevant date.

b) The work must carry prominent notices stating that it is
released under this License and any conditions added under section
7. This requirement modifies the requirement in section 4 to
"keep intact all notices".

c) You must license
the entire work, as a whole, under this
License to anyone who comes into possession of a copy. This
License will therefore apply, along with any applicable section 7
additional terms, to the whole of the work, and all its parts,
regardless of how they are packaged. This License gives no
permission to license the work in any other way, but it does not
invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display
Appropriate Legal Notices; however, if the Program has interactive
interfaces that do not display Appropriate Legal Notices, your
work need not make them do so.

A compilation of a covered work with other separate and independent
works, which are not by their nature extensions of the covered work,
and which are not combined with it such as to form a larger program,
in or on a volume of a storage or distribution medium, is called an
"aggregate" if the compilation and
its resulting copyright are not
used to limit the access or legal rights of the compilation's users
beyond what the individual works permit. Inclusion of a covered work
in an aggregate does not cause this License to apply to the other
parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no

charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object
code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute
modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information
does not include a
requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included
in this License, to the extent
that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections
15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your

receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time
you convey a covered work, the recipient automatically
receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not
impose a license fee, royalty, or other charge for exercise of
rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically

extended to all recipients of the covered
work and works based on it.

A patent license is "discriminatory" if it does not include within
the scope of its coverage, prohibits the exercise of, or is
conditioned on the non-exercise of one or more of the rights that are
specifically granted under this License. You may not convey a covered
work if you are a party to an arrangement with a third party that is
in the business of distributing software, under which you make payment
to the third party based on the extent of your activity of conveying
the work, and under which the third party grants, to any of the
parties who would receive the covered work from you, a discriminatory
patent license (a) in connection with copies of the covered work
conveyed by you (or copies made from those copies), or (b) primarily
for and in connection with specific products or compilations that
contain the covered work, unless you entered into that arrangement,
or that patent license was granted, prior to 28
March 2007.

Nothing in this License shall be construed as excluding or limiting
any implied license or other defenses to infringement that may
otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or
otherwise) that contradict the conditions of this License, they do not
excuse you from the conditions of this License. If you cannot convey a
covered work so as to satisfy simultaneously your obligations under this
License and any other pertinent obligations, then as a consequence you may
not convey it at all. For example, if you agree to terms that obligate you
to collect a royalty for further conveying from those to whom you convey
the Program, the only way you could satisfy both those terms and this
License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License,
you have
permission to link or combine any covered work with a work licensed
under version 3 of the GNU Affero General Public License into a single
combined work, and to convey the resulting work. The terms of this
License will continue to apply to the part which is the covered work,
but the special requirements of the GNU Affero General Public License,
section 13, concerning interaction through a network will apply to the
combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF

SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer
of warranty and limitation of liability provided
above cannot be given local legal effect according to their terms,
reviewing courts shall apply local law that most closely approximates
an absolute waiver of all civil liability in connection with the
Program, unless a warranty or assumption of liability accompanies a
copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest
possible use to the public, the best way to achieve this is to make it
free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest
to attach them to the start of each source file to most effectively
state the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief
idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation, either version 3 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>

This program comes with
ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what you want to do, use the GNU Lesser General
Public License instead of this License. But first,
please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.

1.10 dhcp 4.3.4

1.10.1 Available under license :

Copyright (c) 2004-2015 by Internet Systems Consortium, Inc. ("ISC")
Copyright (c) 1995-2003 by Internet Software Consortium
#
Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.
#
THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES
WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR
ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT
OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.
#
Internet Systems Consortium, Inc.
950 Charter Street
Redwood City, CA 94063
<info@isc.org>
https://www.isc.org/

See the specific source files for

any additional copyright or
license statements.
Redistribution terms Automated Testing Framework
==========

License
****

Copyright (c) 2007, 2008, 2009, 2010, 2011, 2012 The NetBSD Foundation, Inc.
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice,
this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE NETBSD FOUNDATION, INC. AND CONTRIBUTORS
``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED.
IN NO EVENT SHALL THE FOUNDATION OR CONTRIBUTORS
BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

Copyright 2011, 2012 Google Inc.
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation

and/or other materials provided with the distribution.

* Neither the name of Google Inc. nor the names of its contributors
may be used to endorse or promote products derived from this software
without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Relicensed
code
****

The following code snippets have been taken from other projects. Even
though they were not originally licensed under the terms above, the
original authors have agreed to relicense their work so that this project
can be distributed under a single license. This section is put here just to
clarify this fact.

* configure.ac, Makefile.am: The original versions were derived from the
ones in the XML Catalog Manager project, version 2.2.

Author: Julio Merino <jmmv@users.sourceforge.net>

* atf-c/ui.c: The format_paragraph and format_text functions were
derived form the ones in the Monotone project, revision
3a0982da308228d796df35f98d787c5cff2bb5b6.

Author: Julio Merino <jmmv@NetBSD.org>

* atf-c++/detail/io.hpp, atf-c++/detail/io.cpp, atf-c++/detail/io_test.cpp:
These files were derived from the file_handle, systembuf, pipe and pistream
classes and tests found in the Boost.Process library.

Author: Julio Merino <jmmv84@gmail.com>

* admin/check-style.sh,

admin/check-style-common.awk,
admin/check-style-cpp.awk, admin/check-style-shell.awk: These files,
except the first one, were first implemented in the Buildtool project.
They were later adapted to be part of Boost.Process and, during that
process, the shell script was created.

Author: Julio Merino <jmmv84@gmail.com>

==========

vim: filetype=text:textwidth=75:expandtab:shiftwidth=2:softtabstop=2

Copyright (c) 2004-2016 by Internet Systems Consortium, Inc. ("ISC")
Copyright (c) 1995-2003 by Internet Software Consortium
#
Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.
#
THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES
WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR
ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT
OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.
#
Internet Systems Consortium, Inc.
950 Charter Street
Redwood City, CA 94063
<info@isc.org>
https://www.isc.org/

See the specific source files for
 any additional copyright or
license statements.
Copyright (C) 2004-2016 Internet Systems Consortium, Inc. ("ISC")
Copyright (C) 1996-2003 Internet Software Consortium.

Permission to use, copy, modify, and/or distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR

PERFORMANCE OF THIS SOFTWARE.

Portions of this code release fall under one or more of the
following Copyright notices. Please see individual source
files for details.

For binary releases also see: OpenSSL-LICENSE.

Copyright
(C) 1996-2001 Nominum, Inc.

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND NOMINUM DISCLAIMS ALL WARRANTIES
WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL NOMINUM BE LIABLE FOR
ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT
OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (C) 1995-2000 by Network Associates, Inc.

Permission to use, copy, modify, and/or distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright
notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC AND NETWORK ASSOCIATES DISCLAIMS
ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE
FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR
IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (C) 2002 Stichting NLnet, Netherlands, stichting@nlnet.nl.

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the
above copyright notice and this permission notice appear in all
copies.

THE SOFTWARE IS PROVIDED "AS IS" AND STICHTING NLNET
DISCLAIMS ALL WARRANTIES
WITH REGARD TO THIS SOFTWARE INCLUDING ALL
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL
STICHTING NLNET BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR
CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS
OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE
USE OR PERFORMANCE OF THIS SOFTWARE.

The development of Dynamically Loadable Zones (DLZ) for Bind 9 was
conceived and contributed by Rob Butler.

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the
above copyright notice and this permission notice appear in all
copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ROB BUTLER
DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL
ROB BUTLER BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR
CONSEQUENTIAL DAMAGES
OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS
OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE
USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (c) 1987, 1990, 1993, 1994
The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors
may be used to endorse
or promote products derived from this software
without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS" AND

ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (C) The Internet Society 2005. This version of this module is part of RFC 4178; see the RFC itself for full legal notices.

(The above copyright notice is per RFC 3978 5.6 (a), q.v.)

Copyright (c) 2004 Masarykova universita
(Masaryk University, Brno, Czech Republic)
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS

INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1997 - 2003 Kungliga Tekniska Hgskolan
(Royal Institute of Technology, Stockholm, Sweden).
All rights reserved.

Redistribution and use in source and binary forms, with
 or without
modification, are permitted provided that the following conditions
are met:

1. Redistributions of source code must retain the above copyright
  notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.

3. Neither the name of the Institute nor the names of its contributors
  may be used to endorse or promote products derived from this software
  without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE INSTITUTE AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE INSTITUTE OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL

DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

Copyright (c) 1998 Doug Rabson
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

THIS
SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

Copyright ((c)) 2002, Rice University
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the
following conditions are
met:

* Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above
copyright notice, this list of conditions and the following
disclaimer in the documentation and/or other materials provided
with the distribution.

* Neither the name of Rice University (RICE) nor the names of its
contributors may be used to endorse or promote products derived
from this software without specific prior written permission.

This software is provided by RICE and the contributors on an "as is"
basis, without any representations or warranties of any kind, express
or implied including, but not limited to, representations or
warranties of non-infringement, merchantability or fitness for a
particular purpose. In no event shall RICE or contributors be liable
for any direct, indirect, incidental, special, exemplary, or

consequential
damages (including, but not limited to, procurement of
substitute goods or services; loss of use, data, or profits; or
business interruption) however caused and on any theory of liability,
whether in contract, strict liability, or tort (including negligence
or otherwise) arising in any way out of the use of this software, even
if advised of the possibility of such damage.

Copyright (c) 1993 by Digital Equipment Corporation.

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies, and that
the name of Digital Equipment Corporation not be used in advertising or
publicity pertaining to distribution of the document or software without
specific, written prior permission.

THE SOFTWARE IS PROVIDED "AS IS" AND DIGITAL EQUIPMENT CORP. DISCLAIMS ALL
WARRANTIES
WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES
OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL DIGITAL EQUIPMENT
CORPORATION BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL
DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR
PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS
ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS
SOFTWARE.

Copyright 2000 Aaron D. Gifford. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation
and/or other materials provided with the distribution.
3. Neither the name of the copyright holder nor the names of contributors
may be used to endorse or promote products derived from this software
without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR(S) AND CONTRIBUTOR(S) ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE

IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR(S) OR CONTRIBUTOR(S) BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1998 Doug Rabson.
Copyright (c) 2001 Jake Burkholder.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (C) 1995, 1996, 1997, and 1998 WIDE Project.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other
materials provided with the distribution.
3. Neither the name of the project nor the names of its contributors
may be used to endorse or promote products derived from this software
without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

Copyright
(c) 1999-2000 by Nortel Networks Corporation

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND NORTEL NETWORKS DISCLAIMS
ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES
OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL NORTEL NETWORKS
BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES
OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS,
WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION,
ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS
SOFTWARE.

Copyright (c) 2000-2002 Japan Network Information Center. All rights reserved.

By using this file, you agree
to the terms and conditions set forth bellow.

LICENSE TERMS AND CONDITIONS

The following License Terms and Conditions apply, unless a different

license is obtained from Japan Network Information Center ("JPNIC"),
a Japanese association, Kokusai-Kougyou-Kanda Bldg 6F, 2-3-4 Uchi-Kanda,
Chiyoda-ku, Tokyo 101-0047, Japan.

1. Use, Modification and Redistribution (including distribution of any
modified or derived work) in source and/or binary forms is permitted
under this License Terms and Conditions.

2. Redistribution of source code must retain the copyright notices as they
appear in each source code file, this License Terms and Conditions.

3. Redistribution in binary form must reproduce the Copyright Notice,
this License Terms and Conditions, in the documentation and/or other
materials provided with the distribution. For the purposes of binary
distribution the "Copyright Notice" refers to the following language:
"Copyright (c) 2000-2002
Japan Network Information Center. All rights
reserved."

4. The name of JPNIC may not be used to endorse or promote products
derived from this Software without specific prior written approval of
JPNIC.

5. Disclaimer/Limitation of Liability: THIS SOFTWARE IS PROVIDED BY JPNIC
"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL JPNIC BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Copyright
(C) 2004 Nominet, Ltd.

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND NOMINET DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM

LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Portions Copyright RSA Security Inc.

License to copy and use this software is granted provided that it is
identified as "RSA Security Inc.
PKCS #11 Cryptographic Token Interface
(Cryptoki)" in all material mentioning or referencing this software.

License is also granted to make and use derivative works provided that
such works are identified as "derived from the RSA Security Inc. PKCS #11
Cryptographic Token Interface (Cryptoki)" in all material mentioning or
referencing the derived work.

RSA Security Inc. makes no representations concerning either the
merchantability of this software or the suitability of this software for
any particular purpose. It is provided "as is" without express or implied
warranty of any kind.

Copyright (c) 1996, David Mazieres <dm@uun.org>
Copyright (c) 2008, Damien Miller <djm@openbsd.org>

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS
PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES
WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR
ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF
OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (c) 2000-2001 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and
the following disclaimer in
the documentation and/or other materials provided with the
distribution.

3. All advertising materials mentioning features or use of this
software must display the following acknowledgment:
"This product includes software developed by the OpenSSL Project
for use in the OpenSSL Toolkit. (http://www.OpenSSL.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
endorse or promote products derived from this software without
prior written permission. For written permission, please contact
licensing@OpenSSL.org.

5. Products derived from this software may not be called "OpenSSL"
nor may "OpenSSL" appear in their names without prior written
permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following
acknowledgment:
"This product includes software developed by the OpenSSL Project
for use in the OpenSSL Toolkit (http://www.OpenSSL.org/)"

THIS SOFTWARE IS PROVIDED
BY THE OpenSSL PROJECT ``AS IS'' AND ANY
EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1995, 1997, 1998 The NetBSD Foundation, Inc.
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the
following conditions
are met:
1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE NETBSD FOUNDATION, INC. AND CONTRIBUTORS
``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE FOUNDATION OR CONTRIBUTORS
BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.
Copyright (c) 2005 - 2008, Holger Zuleger HZnet. All rights reserved.

This software is open source.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

Redistributions of source code must retain the above copyright notice,
this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice,
this list of conditions and the following disclaimer in the documentation
and/or other materials provided with the distribution.

Neither the name of Holger Zuleger HZnet nor the names of its contributors may
be used to endorse or promote products derived from this software without
specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED.
IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE
LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF

SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
Copyright (c) 2000-2002 Japan Network Information Center. All rights reserved.

By using this file, you agree to the terms and conditions set forth bellow.

LICENSE TERMS AND CONDITIONS

The following License Terms and Conditions apply, unless a different
license is obtained from Japan Network Information Center ("JPNIC"),
a Japanese association, Kokusai-Kougyou-Kanda Bldg 6F, 2-3-4 Uchi-Kanda,
Chiyoda-ku, Tokyo 101-0047, Japan.

1. Use, Modification and Redistribution (including distribution of any
modified or derived work) in source and/or binary forms is permitted
under this License Terms and Conditions.

2. Redistribution of source code must retain the copyright notices as they
appear in each source code file, this License Terms and Conditions.

3. Redistribution in binary form must reproduce the Copyright Notice,
this License Terms and Conditions, in the documentation and/or other
materials provided with the distribution. For the purposes of binary
distribution
the "Copyright Notice" refers to the following language:
"Copyright (c) 2000-2002 Japan Network Information Center. All rights reserved."

4. The name of JPNIC may not be used to endorse or promote products
derived from this Software without specific prior written approval of
JPNIC.

5. Disclaimer/Limitation of Liability: THIS SOFTWARE IS PROVIDED BY JPNIC
"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL JPNIC BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE,
EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

1.11 openssl 1.0.2j

1.11.1 Notifications :

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)
This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).
This product includes software written by Tim Hudson (tjh@cryptsoft.com).

1.11.2 Available under license :

Copyright (C) 1995-1997 Eric Young (eay@cryptsoft.com)
All rights reserved.

This package is an DES implementation written by Eric Young (eay@cryptsoft.com).
The implementation was written so as to conform with MIT's libdes.

This library is free for commercial and non-commercial use as long as
the following conditions are aheared to. The following conditions
apply to all code found in this distribution.

Copyright remains Eric Young's, and as such any Copyright notices in
the code are not to be removed.
If this package is used in a product, Eric Young should be given attribution
as the author of that the SSL library. This can be in the form of a textual
message at program startup or in documentation (online or textual) provided
with the package.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the copyright
  notice, this list of conditions and
 the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software
  must display the following acknowledgement:
  This product includes software developed by Eric Young (eay@cryptsoft.com)

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY,

OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The license and distribution terms for any publically available version or
derivative of this code cannot be changed. i.e. this code cannot simply be
copied and put under another distrubution license
[including the GNU Public License.]

The reason behind this being stated in this direct manner is past
experience in code simply being copied and the attribution removed
from it and then being distributed as part of other packages. This
implementation was a non-trivial and unpaid effort.
Copyright (C) 1995-1997 Eric Young (eay@cryptsoft.com)
All rights reserved.

This package is an Blowfish implementation written
by Eric Young (eay@cryptsoft.com).

This library is free for commercial and non-commercial use as long as
the following conditions are aheared to. The following conditions
apply to all code found in this distribution.

Copyright remains Eric Young's, and as such any Copyright notices in
the code are not to be removed.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software
must display the following acknowledgement:
This product includes software developed by Eric Young (eay@cryptsoft.com)

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF

SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied
and put under another distrubution license
[including the GNU Public License.]

The reason behind this being stated in this direct manner is past experience in code simply being copied and the attribution removed from it and then being distributed as part of other packages. This implementation was a non-trivial and unpaid effort.

LICENSE ISSUES
==========

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

/* ==
* Copyright (c) 1998-2016 The OpenSSL Project. All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
* notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer
in
* the documentation and/or other materials provided with the
* distribution.
*
* 3. All advertising materials mentioning features or use of this
* software must display the following acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
* endorse or promote products derived from this software without

```
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software
 written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/

Original SSLeay License
-----------------------

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to.  The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code.  The SSL documentation
* included with this distribution is covered by the same copyright terms
```

* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the
 library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
*   notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*   notice, this list of conditions and the following disclaimer in the
*   documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*   must display the following acknowledgement:
*   "This product includes cryptographic software written by
*   Eric Young (eay@cryptsoft.com)"
*   The word 'cryptographic' can be left out if the rouines from the library
*   being used are not cryptographic
 related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
*   the apps directory (application code) you must include an acknowledgement:
*   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY
 OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed. i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/

1.12 libxslt 1.1.29

1.12.1 Available under license :

DocBk XML V3.1.7 DTD
Copyright (C) 1998, 1999 Norman Walsh
http://nwalsh.com/docbook/xml/

You may distribute this DTD under the same terms as DocBook.

Please direct all questions and comments about this DTD to
Norman Walsh, <ndw@nwalsh.com>.

This DTD is based on the DocBook V3.1 DTD from OASIS:

[DocBook is] Copyright 1992, 1993, 1994, 1995, 1996, 1998,
1999 HaL Computer Systems, Inc., O'Reilly & Associates, Inc.,
ArborText, Inc., Fujitsu Software Corporation, and the
Organization for the Advancement of Structured Information
Standards (OASIS).

Permission to use, copy, modify and distribute the DocBook
DTD and its accompanying documentation for any purpose and
without fee is hereby granted in perpetuity, provided that
the above copyright notice and this paragraph appear in all
copies. The copyright holders make no representation about
the suitability of the DTD for any purpose. It is provided
"as is" without expressed or implied warranty.

For
more information about the DocBook DTD, see
http://www.oasis-open.org/docbook/
Simplified DocBk XML V3.1.7.1 DTD
Copyright (C) 1999 Norman Walsh
http://nwalsh.com/docbook/simple/

You may distribute this DTD under the same terms as DocBook.

Please direct all questions and comments about this DTD to
Norman Walsh, <ndw@nwalsh.com>.

This DTD is based on the DocBk XML DTD, which is in turn based
on the DocBook V3.1 DTD from OASIS:

[DocBook is] Copyright 1992, 1993, 1994, 1995, 1996, 1998,
1999 HaL Computer Systems, Inc., O'Reilly & Associates, Inc.,
ArborText, Inc., Fujitsu Software Corporation, and the

Organization for the Advancement of Structured Information
Standards (OASIS).

Permission to use, copy, modify and distribute the DocBook
DTD and its accompanying documentation for any purpose and
without fee is hereby granted in perpetuity, provided that
the above copyright notice and this paragraph appear in all
copies. The copyright holders make no representation about
the suitability of the DTD for any purpose. It is
provided
"as is" without expressed or implied warranty.

For more information about the DocBook DTD, see
http://www.oasis-open.org/docbook/
Licence for libxslt except libexslt

Copyright (C) 2001-2002 Daniel Veillard. All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is fur-
nished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FIT-
NESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
DANIEL VEILLARD BE LIABLE
FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER
IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CON-
NECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of Daniel Veillard shall not
be used in advertising or otherwise to promote the sale, use or other deal-
ings in this Software without prior written authorization from him.

Licence for libexslt

Copyright (C) 2001-2002 Thomas Broyer, Charlie Bozeman and Daniel Veillard.
All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy

of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense,
 and/or sell
copies of the Software, and to permit persons to whom the Software is fur-
nished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FIT-
NESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER
IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CON-
NECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of the authors shall not
be used in advertising or otherwise to promote the sale, use or other deal-
ings in this Software without prior written authorization from him.

Copyright

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the Software), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

Except as contained in this notice, the names of individuals credited with contribution to this software shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization from the individuals in question.

Any stylesheet derived from this Software that is publically distributed will be identified with a different name and the version strings
 in any derived Software will be changed so that no possibility of confusion between the derived package and this Software will exist.
Simplified DocBook XML V4.1.2.4 DTD
Copyright (C) 1999, 2000 Norman Walsh
http://nwalsh.com/docbook/simple/

You may distribute this DTD under the same terms as DocBook.

Please direct all questions and comments about this DTD to
Norman Walsh, <ndw@nwalsh.com>.

This DTD is based on the DocBook XML V4.1.2 DTD from OASIS:

[DocBook is] Copyright 1992-2000 HaL Computer Systems, Inc.,
O'Reilly & Associates, Inc., ArborText, Inc., Fujitsu Software
Corporation, Norman Walsh, and the Organization for the
Advancement of Structured Information Standards (OASIS).

Permission to use, copy, modify and distribute the DocBook
DTD and its accompanying documentation for any purpose and
without fee is hereby granted in perpetuity, provided that
the above copyright notice and this paragraph appear in all
copies. The copyright holders make no representation about
the suitability of the DTD for any purpose. It is provided
"as is" without expressed or implied warranty.

For
more information about the DocBook DTD, see
http://www.oasis-open.org/docbook/

1.13 glib 2.48.2

1.13.1 Available under license :

This work may be reproduced and distributed in whole or in part, in
any medium, physical or electronic, so as long as this copyright
notice remains intact and unchanged on all copies. Commercial
redistribution is permitted and encouraged, but you may not
redistribute, in whole or in part, under terms more restrictive than
those under which you received it. If you redistribute a modified or
translated version of this work, you must also make the source code to
the modified or translated version available in electronic form
without charge. However, mere aggregation as part of a larger work
shall not count as a modification for this purpose.

All code examples in this work are placed into the public domain,
and may be used, modified and redistributed without restriction.

BECAUSE THIS WORK IS LICENSED FREE OF CHARGE, THERE IS NO
WARRANTY FOR THE WORK, TO THE EXTENT PERMITTED BY APPLICABLE LAW.
EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR
OTHER PARTIES PROVIDE THE
WORK "AS IS" WITHOUT WARRANTY OF ANY
KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE. SHOULD THE WORK PROVE DEFECTIVE, YOU ASSUME
THE COST OF ALL NECESSARY REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN

WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE WORK AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE WORK, EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
PCRE LICENCE

Please see the file LICENCE in the PCRE distribution for licensing details.

End
GNU LIBRARY GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the library GPL. It is
numbered 2 because it goes with version 2 of the ordinary GPL.]

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
Licenses are intended to guarantee your freedom to share and change
free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some
specially designated Free Software Foundation software, and to any
other libraries whose authors decide to use it. You can use it for
your libraries, too.

When we speak of free software, we are referring
to freedom, not
price. Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid
anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate to certain responsibilities for you if
you distribute copies of the library, or if you modify it.

For example, if you distribute copies of the library, whether gratis

or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link a program with the library, you must provide complete object files to the recipients so that they can relink them with the library, after making
changes to the library and recompiling
it. And you must show them these terms so they know their rights.

Our method of protecting your rights has two steps: (1) copyright the library, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the library.

Also, for each distributor's protection, we want to make certain that everyone understands that there is no warranty for this free library. If the library is modified by someone else and passed on, we want its recipients to know that what they have is not the original version, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that companies distributing free software will individually obtain patent licenses, thus in effect transforming the program into proprietary software. To prevent this, we have made it clear that any patent must
be licensed for everyone's
free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License, which was designed for utility programs. This license, the GNU Library General Public License, applies to certain designated libraries. This license is quite different from the ordinary one; be sure to read it in full, and don't assume that anything in it is the same as in the ordinary license.

The reason we have a separate public license for some libraries is that they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and legal sense, the linked executable is a combined work, a derivative of the original library, and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public License for libraries did not effectively promote software sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

GNU LIBRARY GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent
of the use of the Library in a tool for
writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work
must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by

this function must
be optional: if the application does not supply it, the square
root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In
addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code
of
the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a

medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also compile or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

c) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

d) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you

distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or

otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not
distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system;
it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Library General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or
concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by

the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year>
<name of author>

This library is free software; you can redistribute it and/or
modify it under the terms of the GNU Library General Public
License as published by the Free Software Foundation; either
version 2 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
Library General Public License for more details.

You should have received a copy of the GNU Library General Public
License along with this library; if not, write to the
Free Software Foundation, Inc., 59 Temple Place - Suite 330,
Boston, MA 02111-1307 USA.

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary.
Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the
library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

1.14 glibc 2.24

1.14.1 Available under license :

Copyright 1992, 1993, 1994, 1997 Henry Spencer. All rights reserved.
This software is not subject to any license of the American Telephone
and Telegraph Company or of the Regents of the University of California.

Permission is granted to anyone to use this software for any purpose on

any computer system, and to alter it and redistribute it, subject
to the following restrictions:

1. The author is not responsible for the consequences of use of this
  software, no matter how awful, even if they arise from flaws in it.

2. The origin of this software must not be misrepresented, either by
  explicit claim or by omission. Since few users ever read sources,
  credits must appear in the documentation.

3. Altered versions must be plainly marked as such, and must not be
  misrepresented as being the original software. Since few users
  ever read sources, credits must appear in the documentation.

4. This notice may not be removed or altered.

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts
as the successor of the GNU Library Public License, version 2, hence
the version number 2.1.]

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
Licenses are intended to guarantee your freedom to share and change
free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some
specially designated software packages--typically libraries--of the
Free Software Foundation and other authors who
decide to use it. You
can use it too, but we suggest you first think carefully about whether
this license or the ordinary General Public License is the better
strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use,
not price. Our General Public Licenses are designed to make sure that
you have the freedom to distribute copies of free software (and charge
for this service if you wish); that you receive source code or can get
it if you want it; that you can change the software and use pieces of
it in new free programs; and that you are informed that you can do

these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General

Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices

stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the
terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be
reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary
GNU General Public
License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2,

instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline

functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the
object code for the work under the terms of Section 6.
Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany
the work with the complete corresponding
machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate
properly with a modified version of the library, if
the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at
least three years, to give the same user the materials
specified in Subsection 6a, above, for a charge no more
than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy
from a designated place, offer equivalent access to copy the above
specified materials from the same place.

e) Verify that the user has already received a copy of these
materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the
Library" must include any data and utility programs needed for
reproducing the executable from it. However, as a special exception,
the materials to be distributed need not include anything that is
normally
distributed (in either source or binary form) with the major
components (compiler, kernel, and so on) of the operating system on
which the executable runs, unless that component itself accompanies
the executable.

It may happen that this requirement contradicts the license
restrictions of other proprietary libraries that do not normally
accompany the operating system. Such a contradiction means you cannot
use both them and the Library together in an executable that you
distribute.

7. You may place library facilities that are a work based on the
Library side-by-side in a single library together with other library
facilities not covered by this License, and distribute such a combined
library, provided that the separate distribution of the work based on
the Library and of the other library facilities is otherwise
permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work
based on the Library, uncombined with any
other library
facilities. This must be distributed under the terms of the
Sections above.

b) Give prominent notice with the combined library of the fact
that part of it is a work based on the Library, and explaining
where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute
the Library except as expressly provided under this License. Any
attempt otherwise to copy, modify, sublicense, link with, or

distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if
you do not accept this License. Therefore, by
modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse
you from the conditions of this License. If you cannot
distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system
which is
implemented by public license practices. Many people have made generous contributions to the wide range of software distributed

through that system in reliance on consistent application of that
system; it is up to the author/donor to decide if he or she is willing
to distribute software through any other system and a licensee cannot
impose that choice.

This section is intended to make thoroughly clear what is believed to
be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in
certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Library under this License may add
an explicit geographical distribution limitation excluding those countries,
so that distribution is permitted only in or among countries not thus
excluded. In such case, this License incorporates the limitation as if
written in the body of this License.

13. The Free Software Foundation may publish
revised and/or new
versions of the Lesser General Public License from time to time.
Such new versions will be similar in spirit to the present version,
but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library
specifies a version number of this License which applies to it and
"any later version", you have the option of following the terms and
conditions either of that version or of any later version published by
the Free Software Foundation. If the Library does not specify a
license version number, you may choose any version ever published by
the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free
programs whose distribution conditions are incompatible with these,
write to the author to ask for permission. For software which is
copyrighted by the Free Software Foundation, write to the Free
Software Foundation; we sometimes make exceptions for this. Our
decision
will be guided by the two goals of preserving the free status
of all derivatives of our free software and of promoting the sharing
and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO
WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW.
EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR
OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY
KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR

PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE,
BE LIABLE TO YOU
FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey
the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301

USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the library, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the
library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

1.15 python 2.7.12

1.15.1 Available under license :

Copyright (c) 2002 Jorge Acereda <jacereda@users.sourceforge.net> &
Peter O'Gorman <ogorman@users.sourceforge.net>

Portions may be copyright others, see the AUTHORS file included with this
distribution.

Maintained by Peter O'Gorman <ogorman@users.sourceforge.net>

Bug Reports and other queries should go to <ogorman@users.sourceforge.net>

Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY
KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE
LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION

OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
libffi - Copyright (c) 1996-2003 Red Hat, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the ``Software''), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED ``AS IS'', WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL CYGNUS SOLUTIONS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH
THE SOFTWARE OR THE USE OR
OTHER DEALINGS IN THE SOFTWARE.
X Window System License - X11R6.4

Copyright (c) 1998 The Open Group

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE OPEN GROUP BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION
WITH THE SOFTWARE OR THE USE OR
OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of The Open Group shall

not be used in advertising or otherwise to promote the sale, use or
other dealings in this Software without prior written authorization
from The Open Group.

X Window System is a trademark of The Open Group
portions copyright 2001, Autonomous Zones Industries, Inc., all rights...
err... reserved and offered to the public under the terms of the
Python 2.2 license.
Author: Zooko O'Whielacronx
http://zooko.com/
mailto:zooko@zooko.com
#
Copyright 2000, Mojam Media, Inc., all rights reserved.
Author: Skip Montanaro
#
Copyright 1999, Bioreason, Inc., all rights reserved.
Author: Andrew Dalke
#
Copyright 1995-1997, Automatrix, Inc., all rights reserved.
Author: Skip Montanaro
#
Copyright 1991-1995, Stichting Mathematisch Centrum, all rights reserved.
#
#
Permission to use, copy, modify, and distribute this Python software and
its associated documentation for any purpose without fee is hereby
granted, provided that the above copyright notice appears in all copies,
and that both that copyright notice and this permission notice appear in
supporting documentation, and that the name of neither Automatrix,
Bioreason or Mojam Media be used in
 advertising or publicity pertaining to
distribution of the software without specific, written prior permission.
pybench License

This copyright notice and license applies to all files in the pybench
directory of the pybench distribution.

Copyright (c), 1997-2006, Marc-Andre Lemburg (mal@lemburg.com)
Copyright (c), 2000-2006, eGenix.com Software GmbH (info@egenix.com)

All Rights Reserved.

Permission to use, copy, modify, and distribute this software and its
documentation for any purpose and without fee or royalty is hereby
granted, provided that the above copyright notice appear in all copies
and that both that copyright notice and this permission notice appear
in supporting documentation or portions thereof, including

modifications, that you make.

THE AUTHOR MARC-ANDRE LEMBURG DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING

FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE !
Additional Conditions for this Windows binary build

This program is linked with and uses Microsoft Distributable Code, copyrighted by Microsoft Corporation. The Microsoft Distributable Code includes the following files:

msvcr90.dll
msvcp90.dll
msvcm90.dll

If you further distribute programs that include the Microsoft Distributable Code, you must comply with the restrictions on distribution specified by Microsoft. In particular, you must require distributors and external end users to agree to terms that protect the Microsoft Distributable Code at least as much as Microsoft's own requirements for the Distributable Code. See Microsoft's documentation (included in its developer tools and on its website at microsoft.com) for specific details.

Redistribution of the Windows binary build of the Python interpreter complies with this agreement, provided that you do not:

- alter any copyright, trademark
or patent notice in Microsoft's
Distributable Code;

- use Microsoft's trademarks in your programs' names or in a way that suggests your programs come from or are endorsed by Microsoft;

- distribute Microsoft's Distributable Code to run on a platform other than Microsoft operating systems, run-time technologies or application platforms; or

- include Microsoft Distributable Code in malicious, deceptive or unlawful programs.

These restrictions apply only to the Microsoft Distributable Code as

defined above, not to Python itself or any programs running on the
Python interpreter. The redistribution of the Python interpreter and
libraries is governed by the Python Software License included with this
file, or by other licenses as marked.
""" robotparser.py

  Copyright (C) 2000 Bastian Kleineidam

  You can choose between two licenses when using this package:
  1) GNU GPLv2
  2) PSF license for Python 2.2
#---
Copyright (c) 1997-2001 by Total Control Software
All Rights Reserved
#---
#
Module Name: dbShelve.py
#
Description: A reimplementation of the standard shelve.py that
forces the use of cPickle, and DB.
#
Creation Date: 11/3/97 3:39:04PM
#
License: This is free software. You may use this software for any
purpose including modification/redistribution, so long as
this header remains intact and that you do not claim any
rights of ownership or authorship of this software. This
software has been tested, but no warranty is expressed or
implied.
/* --

 unicodedata -- Provides access to the Unicode 5.1 data base.

 Data was extracted from the Unicode 5.1 UnicodeData.txt file.

 Written by Marc-Andre Lemburg (mal@lemburg.com).
 Modified for Python 2.0 by Fredrik Lundh (fredrik@pythonware.com)
 Modified by Martin v. L"wis (martin@v.loewis.de)

 Copyright (c) Corporation for National Research Initiatives.

 -- */
Copyright 2007 Google, Inc. All Rights Reserved.
Licensed to PSF under a Contributor Agreement.
/*
Copyright (c) 2002 Jorge Acereda <jacereda@users.sourceforge.net> &
               Peter O'Gorman <ogorman@users.sourceforge.net>

Portions may be copyright others, see the AUTHORS file included with this
distribution.

Maintained by Peter O'Gorman <ogorman@users.sourceforge.net>

Bug Reports and other queries should go to <ogorman@users.sourceforge.net>

Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE
LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION
WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
*/
Copyright (c) 1998-2002 John Aycock
#
Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:
#
The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.
#
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.
IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY
CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN
ACTION OF CONTRACT,
TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE

/* Random objects */

/* --
The code in this module was based on a download from:
http://www.math.keio.ac.jp/~matumoto/MT2002/emt19937ar.html

It was modified in 2002 by Raymond Hettinger as follows:

* the principal computational lines untouched except for tabbing.

* renamed genrand_res53() to random_random() and wrapped
in python calling/return code.

* genrand_int32() and the helper functions, init_genrand()
and init_by_array(), were declared static, wrapped in
Python calling/return code. also, their global data
references were replaced with structure references.

* unused functions from the original were deleted.
new, original C python code was added to implement the
Random() interface.

The following are the verbatim comments from the original code:

A C-program for MT19937, with initialization improved 2002/1/26.
Coded by Takuji Nishimura and Makoto Matsumoto.

Before using, initialize the state by using init_genrand(seed)
or init_by_array(init_key, key_length).

Copyright (C) 1997 - 2002, Makoto Matsumoto and Takuji Nishimura,
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

3. The names of its contributors may not be used to endorse or promote
products derived from this software without specific prior written
permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
"AS IS" AND ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR
PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Any feedback is very welcome.
http://www.math.keio.ac.jp/matumoto/emt.html
email: matumoto@math.keio.ac.jp
*/

A. HISTORY OF THE SOFTWARE
==========

Python was created in the early 1990s by Guido van Rossum at Stichting
Mathematisch Centrum (CWI, see http://www.cwi.nl) in the Netherlands
as a successor of a language called ABC. Guido remains Python's
principal author, although it includes many contributions from others.

In 1995, Guido continued his work on Python at the Corporation for
National Research Initiatives (CNRI, see http://www.cnri.reston.va.us)
in Reston, Virginia where he released several versions of the
software.

In May 2000, Guido and the Python core development team moved to
BeOpen.com to form the BeOpen PythonLabs team. In October of the same
year, the PythonLabs team moved to Digital Creations (now Zope
Corporation, see http://www.zope.com). In 2001, the Python Software
Foundation (PSF, see http://www.python.org/psf/) was formed, a
non-profit organization created specifically to own Python-related
Intellectual Property. Zope Corporation is a sponsoring member
of
the PSF.

All Python releases are Open Source (see http://www.opensource.org for
the Open Source Definition). Historically, most, but not all, Python
releases have also been GPL-compatible; the table below summarizes
the various releases.

Release Derived Year Owner GPL-

	from		compatible? (1)
0.9.0 thru 1.2		1991-1995	CWI yes
1.3 thru 1.5.2	1.2	1995-1999	CNRI yes
1.6	1.5.2	2000	CNRI no
2.0	1.6	2000	BeOpen.com no
1.6.1	1.6	2001	CNRI yes (2)
2.1	2.0+1.6.1	2001	PSF no
2.0.1	2.0+1.6.1	2001	PSF yes
2.1.1	2.1+2.0.1	2001	PSF yes
2.1.2	2.1.1	2002	PSF yes
2.1.3	2.1.2	2002	PSF yes
2.2 and above			
2.1.1	2001-now		PSF yes

Footnotes:

(1) GPL-compatible doesn't mean that we're distributing Python under the GPL. All Python licenses, unlike the GPL, let you distribute a modified version without making your changes open source. The GPL-compatible licenses make it possible to combine Python with other software that is released under the GPL; the others don't.

(2) According to Richard Stallman, 1.6.1 is not GPL-compatible, because its license has a choice of law clause. According to CNRI, however, Stallman's lawyer has told CNRI's lawyer that 1.6.1 is "not incompatible" with the GPL.

Thanks to the many outside volunteers who have worked under Guido's direction to make these releases possible.

B. TERMS AND CONDITIONS FOR ACCESSING OR OTHERWISE USING PYTHON
==========

PYTHON SOFTWARE FOUNDATION LICENSE VERSION 2
---

1. This LICENSE AGREEMENT
is between the Python Software Foundation
("PSF"), and the Individual or Organization ("Licensee") accessing and otherwise using this software ("Python") in source or binary form and its associated documentation.

2. Subject to the terms and conditions of this License Agreement, PSF hereby grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python alone or in any derivative version,

provided, however, that PSF's License Agreement and PSF's notice of copyright, i.e., "Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016 Python Software Foundation; All Rights Reserved" are retained in Python alone or in any derivative version prepared by Licensee.

3. In the event Licensee prepares a derivative work that is based on or incorporates Python or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python.

4. PSF is making Python available to Licensee on an "AS IS" basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.

7. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSF trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.

8. By copying, installing or otherwise using Python, Licensee agrees to be bound by the terms and conditions of this License Agreement.

BEOPEN.COM LICENSE AGREEMENT FOR PYTHON 2.0

BEOPEN PYTHON OPEN SOURCE LICENSE AGREEMENT VERSION 1

1. This LICENSE AGREEMENT is between BeOpen.com ("BeOpen"), having an office at 160 Saratoga Avenue, Santa Clara, CA 95051, and the Individual or Organization ("Licensee") accessing and otherwise using

this software in source or binary form and its associated
documentation ("the Software").

2. Subject to the terms and conditions of this BeOpen Python License
Agreement, BeOpen hereby grants Licensee a non-exclusive,
royalty-free, world-wide license to reproduce, analyze, test, perform
and/or display publicly,
prepare derivative works, distribute, and
otherwise use the Software alone or in any derivative version,
provided, however, that the BeOpen Python License is retained in the
Software, alone or in any derivative version prepared by Licensee.

3. BeOpen is making the Software available to Licensee on an "AS IS"
basis. BEOPEN MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR
IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, BEOPEN MAKES NO AND
DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS
FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE SOFTWARE WILL NOT
INFRINGE ANY THIRD PARTY RIGHTS.

4. BEOPEN SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF THE
SOFTWARE FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS
AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THE SOFTWARE, OR ANY
DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

5. This License Agreement will automatically terminate upon a material
breach of its terms and conditions.

6.
This License Agreement shall be governed by and interpreted in all
respects by the law of the State of California, excluding conflict of
law provisions. Nothing in this License Agreement shall be deemed to
create any relationship of agency, partnership, or joint venture
between BeOpen and Licensee. This License Agreement does not grant
permission to use BeOpen trademarks or trade names in a trademark
sense to endorse or promote products or services of Licensee, or any
third party. As an exception, the "BeOpen Python" logos available at
http://www.pythonlabs.com/logos.html may be used according to the
permissions granted on that web page.

7. By copying, installing or otherwise using the software, Licensee
agrees to be bound by the terms and conditions of this License
Agreement.

CNRI LICENSE AGREEMENT FOR PYTHON 1.6.1
---

1. This LICENSE AGREEMENT is between the Corporation for National

Research Initiatives, having an office at 1895 Preston
White Drive,
Reston, VA 20191 ("CNRI"), and the Individual or Organization
("Licensee") accessing and otherwise using Python 1.6.1 software in
source or binary form and its associated documentation.

2. Subject to the terms and conditions of this License Agreement, CNRI
hereby grants Licensee a nonexclusive, royalty-free, world-wide
license to reproduce, analyze, test, perform and/or display publicly,
prepare derivative works, distribute, and otherwise use Python 1.6.1
alone or in any derivative version, provided, however, that CNRI's
License Agreement and CNRI's notice of copyright, i.e., "Copyright (c)
1995-2001 Corporation for National Research Initiatives; All Rights
Reserved" are retained in Python 1.6.1 alone or in any derivative
version prepared by Licensee. Alternately, in lieu of CNRI's License
Agreement, Licensee may substitute the following text (omitting the
quotes): "Python 1.6.1 is made available subject to the terms and
conditions in CNRI's License Agreement. This Agreement
together with
Python 1.6.1 may be located on the Internet using the following
unique, persistent identifier (known as a handle): 1895.22/1013. This
Agreement may also be obtained from a proxy server on the Internet
using the following URL: http://hdl.handle.net/1895.22/1013".

3. In the event Licensee prepares a derivative work that is based on
or incorporates Python 1.6.1 or any part thereof, and wants to make
the derivative work available to others as provided herein, then
Licensee hereby agrees to include in any such work a brief summary of
the changes made to Python 1.6.1.

4. CNRI is making Python 1.6.1 available to Licensee on an "AS IS"
basis. CNRI MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR
IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, CNRI MAKES NO AND
DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS
FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON 1.6.1 WILL NOT
INFRINGE ANY THIRD PARTY RIGHTS.

5. CNRI SHALL NOT BE LIABLE TO LICENSEE
OR ANY OTHER USERS OF PYTHON
1.6.1 FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS
A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON 1.6.1,
OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

6. This License Agreement will automatically terminate upon a material
breach of its terms and conditions.

7. This License Agreement shall be governed by the federal
intellectual property law of the United States, including without

limitation the federal copyright law, and, to the extent such
U.S. federal law does not apply, by the law of the Commonwealth of
Virginia, excluding Virginia's conflict of law provisions.
Notwithstanding the foregoing, with regard to derivative works based
on Python 1.6.1 that incorporate non-separable material that was
previously distributed under the GNU General Public License (GPL), the
law of the Commonwealth of Virginia shall govern this License
Agreement only as to issues arising under or with respect to
Paragraphs
4, 5, and 7 of this License Agreement. Nothing in this
License Agreement shall be deemed to create any relationship of
agency, partnership, or joint venture between CNRI and Licensee. This
License Agreement does not grant permission to use CNRI trademarks or
trade name in a trademark sense to endorse or promote products or
services of Licensee, or any third party.

8. By clicking on the "ACCEPT" button where indicated, or by copying,
installing or otherwise using Python 1.6.1, Licensee agrees to be
bound by the terms and conditions of this License Agreement.

ACCEPT

CWI LICENSE AGREEMENT FOR PYTHON 0.9.0 THROUGH 1.2

Copyright (c) 1991 - 1995, Stichting Mathematisch Centrum Amsterdam,
The Netherlands. All rights reserved.

Permission to use, copy, modify, and distribute this software and its
documentation for any purpose and without fee is hereby granted,
provided that the above copyright notice appear in all copies and
that
both that copyright notice and this permission notice appear in
supporting documentation, and that the name of Stichting Mathematisch
Centrum or CWI not be used in advertising or publicity pertaining to
distribution of the software without specific, written prior
permission.

STICHTING MATHEMATISCH CENTRUM DISCLAIMS ALL WARRANTIES WITH REGARD TO
THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND
FITNESS, IN NO EVENT SHALL STICHTING MATHEMATISCH CENTRUM BE LIABLE
FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT
OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

-- abs.decTest -- decimal absolute value --

-- Copyright (c) IBM Corporation, 1981, 2008. All rights reserved. --
---
portions copyright 2001, Autonomous Zones Industries, Inc., all rights...
err... reserved and offered to the public under the terms of the
Python 2.2 license.
Author: Zooko O'Whielacronx
http://zooko.com/
mailto:zooko@zooko.com
#
Copyright 2000, Mojam Media, Inc., all rights reserved.
Author: Skip Montanaro
#
Copyright 1999, Bioreason, Inc., all rights reserved.
Author: Andrew Dalke
#
Copyright 1995-1997, Automatrix, Inc., all rights reserved.
Author: Skip Montanaro
#
Copyright 1991-1995, Stichting Mathematisch Centrum, all rights reserved.
#
#
Permission to use, copy, modify, and distribute this Python software and
its associated documentation for any purpose without fee is hereby
granted, provided that the above copyright notice appears in all copies,
and that both that copyright notice and this permission notice appear in
supporting documentation, and that the name of neither Automatrix,

Bioreason or Mojam Media be used in advertising or publicity pertaining to
distribution of the software without specific, written prior permission.
#
Name: CP1140
Unicode version: 3.2
Table version: 1.0
Table format: Format A
Date: 2005-10-25
Authors: Marc-Andre Lemburg <mal@egenix.com>
#
This encoding is a modified CP037 encoding (with added Euro
currency sign).
#
(c) Copyright Marc-Andre Lemburg, 2005.
Licensed to PSF under a Contributor Agreement.
#
Based on the file
ftp://ftp.unicode.org/Public/MAPPINGS/VENDORS/MICSFT/EBCDIC/CP037.TXT
which is:
#
Copyright (c) 2002 Unicode, Inc. All Rights reserved.

```
#
# This file is provided as-is by Unicode, Inc. (The Unicode Consortium).
# No claims are made as to fitness for any particular purpose.  No
# warranties of any kind are expressed or implied.  The recipient
# agrees to determine applicability of information provided.  If this
# file has been provided on optical media by Unicode, Inc., the sole
# remedy for any claim
 will be exchange of defective media within 90
# days of receipt.
#
# Unicode, Inc. hereby grants the right to freely use the information
# supplied in this file in the creation of products supporting the
# Unicode Standard, and to make copies of this file in any form for
# internal or external distribution as long as this notice remains
# attached.
# '$echo "$cfgfile" | sed 's%^.*/%%" - Provide generalized library-building support services.
# Generated automatically by $PROGRAM (GNU $PACKAGE $VERSION$TIMESTAMP)
# NOTE: Changes made to this file will be lost: look at ltmain.sh.
#
# Copyright (C) 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007
# Free Software Foundation, Inc.
#
# This file is part of GNU Libtool:
# Originally by Gordon Matzigkeit <gord@gnu.ai.mit.edu>, 1996
#
# This program is free software; you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation; either version 2 of the License, or
# (at your option) any later version.
#
# This program is distributed in the hope that it will be useful, but
# WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the GNU
# General Public License for more details.

#
# You should have received a copy of the GNU General Public License
# along with this program; if not, write to the Free Software
# Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.
#
# As a special exception to the GNU General Public License, if you
# distribute this file as part of a program that contains a
# configuration script generated by Autoconf, you may include it under
# the same distribution terms that you use for the rest of that program.
# (C) Copyright 2001  Autonomous Zone Industries
#
# License:  This is free software.  You may use this software for any
#           purpose including modification/redistribution, so long as
```

```
#          this header remains intact and that you do not claim any
#          rights of ownership or authorship of this software.  This
#          software has been tested, but no warranty is expressed or
#          implied.
# subprocess - Subprocesses with accessible I/O streams
#
# For more information about this module, see PEP 324.
#
# This module should remain compatible with Python 2.2, see PEP 291.
#
# Copyright (c) 2003-2005 by Peter Astrand <astrand@lysator.liu.se>
#
# Licensed to PSF under a Contributor Agreement.
# See http://www.python.org/2.4/license for licensing details.
/* -----------------------------------------------------------------------
  ffi.c - Copyright (c) 1998 Cygnus Solutions
         Copyright (c) 2004 Simon Posnjak
    Copyright (c) 2005 Axis Communications AB
    Copyright (C) 2007 Free Software Foundation, Inc.

  CRIS Foreign Function Interface

  Permission is hereby granted, free of charge, to any person obtaining
  a copy of this software and associated documentation files (the
  "Software"), to deal in the Software without restriction, including
  without limitation the rights to use, copy, modify, merge, publish,
  distribute, sublicense, and/or sell copies of the Software, and to
  permit persons to whom the Software is furnished to do so, subject to
  the following conditions:

  The above copyright notice and this permission notice shall be included
  in all copies or substantial portions of the Software.

  THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS
  OR IMPLIED,
 INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
  MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.
  IN NO EVENT SHALL SIMON POSNJAK BE LIABLE FOR ANY CLAIM, DAMAGES OR
  OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE,
  ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR
  OTHER DEALINGS IN THE SOFTWARE.
  ----------------------------------------------------------------------- */
/* -----------------------------------------------------------------------
  ffi.c - Copyright (c) 2004  Renesas Technology
         Copyright (c) 2008  Red Hat, Inc.

  M32R Foreign Function Interface
```

Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be included
in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS
OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR
PURPOSE AND NONINFRINGEMENT.
IN NO EVENT SHALL RENESAS TECHNOLOGY BE LIABLE FOR ANY CLAIM, DAMAGES OR
OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE,
ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR
OTHER DEALINGS IN THE SOFTWARE.
-- */

ElementTree
$Id: ElementInclude.py 1862 2004-06-18 07:31:02Z Fredrik $
#
limited xinclude support for element trees
#
history:
2003-08-15 fl   created
2003-11-14 fl   fixed default loader
#
Copyright (c) 2003-2004 by Fredrik Lundh. All rights reserved.
#
fredrik@pythonware.com
http://www.pythonware.com
#
--
The ElementTree toolkit is
#
Copyright (c) 1999-2004 by Fredrik Lundh
#
By obtaining, using, and/or copying this software and/or its
associated documentation, you agree that you have read, understood,
and will comply with the following terms and conditions:
#
Permission to use, copy, modify, and distribute this software and
its associated documentation for any purpose and without fee is
hereby granted, provided that the above copyright notice appears in
all copies, and that both that copyright notice and

this permission
notice appear in supporting documentation, and that the name of
Secret Labs AB or the author not be used in advertising or publicity
pertaining to distribution of the software without specific, written
prior permission.
#
SECRET LABS AB AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD
TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANT-
ABILITY AND FITNESS. IN NO EVENT SHALL SECRET LABS AB OR THE AUTHOR
BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY
DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS,
WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS
ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE
OF THIS SOFTWARE.
--
libffi - Copyright (c) 1996-2008 Red Hat, Inc and others.
See source files for details.

Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be included
in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.
IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY
CLAIM, DAMAGES OR
 OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT,
TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
install - install a program, script, or datafile
#
This originates from X11R5 (mit/util/scripts/install.sh), which was
later released in X11R6 (xc/config/util/install.sh) with the
following copyright and license.
#
Copyright (C) 1994 X Consortium
#
Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to
deal in the Software without restriction, including without limitation the

```
# rights to use, copy, modify, merge, publish, distribute, sublicense, and/or
# sell copies of the Software, and to permit persons to whom the Software is
# furnished to do so, subject to the following conditions:
#
# The above copyright notice and this permission notice shall be included in
# all copies or substantial portions of the Software.
#
# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
# IMPLIED, INCLUDING BUT NOT
 LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
# FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.  IN NO EVENT SHALL THE
# X CONSORTIUM BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN
# AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNEC-
# TION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
#
# Except as contained in this notice, the name of the X Consortium shall not
# be used in advertising or otherwise to promote the sale, use or other deal-
# ings in this Software without prior written authorization from the X Consor-
# tium.
#
#
# FSF changes to this file are in the public domain.
/* microprotocols.c - minimalist and non-validating protocols implementation
*
* Copyright (C) 2003-2004 Federico Di Gregorio <fog@debian.org>
*
* This file is part of psycopg and was adapted for pysqlite. Federico Di
* Gregorio gave the permission to use it within pysqlite under the following
* license:
*
* This software is provided 'as-is', without any express or implied
* warranty.  In no event will the authors be held liable for any damages
* arising from the use of this software.
*
* Permission is granted to anyone to use this software for any purpose,
* including commercial applications, and to alter it and redistribute it
* freely, subject to the following restrictions:
*
* 1. The origin of this software must not be misrepresented; you must not
*    claim that you wrote the original software. If you use this software
*    in a product, an acknowledgment in the product documentation would be
*    appreciated but is not required.

* 2. Altered source versions must be plainly marked as such, and must not be
*    misrepresented as being the original software.
* 3. This notice may not be removed or altered from any source distribution.
*/
```

```
# Copyright (C) 2000, 2001 by Autonomous Zone Industries
# Copyright (C) 2002 Gregory P. Smith
#
# March 20, 2000
#
# License:      This is free software.  You may use this software for any
#               purpose including modification/redistribution, so long as
#               this header remains intact and that you do not claim any
#               rights of ownership or authorship of this software.  This
#               software has been tested, but no warranty is expressed or
#               implied.
#
#   --  Gregory P. Smith <greg@krypto.org>
#
# $Id: test_dbtables.py 66088 2008-08-31 14:00:51Z jesus.cea $
# Original version written by Greg Stein (gstein@lyra.org)
#                         and Bill Tutt (rassilon@lima.mudlib.org)
# February 1997.
#
# Modifications and improvements for Python 2.0 by Jeremy Hylton and
# Mark Hammond
#
# Some fixes to try to have correct line number on almost all nodes
# (except Module, Discard and Stmt) added by Sylvain Thenault
#
# Portions of this file are:
# Copyright (C) 1997-1998 Greg Stein. All Rights Reserved.
#
# This module is provided under a BSD-ish license. See
#   http://www.opensource.org/licenses/bsd-license.html
# and replace OWNER, ORGANIZATION, and YEAR as appropriate.
#-------------------------------------------------------------------
# tarfile.py
#-------------------------------------------------------------------
# Copyright (C) 2002 Lars Gust?bel <lars@gustaebel.de>
# All rights reserved.
#
# Permission  is  hereby granted,  free  of charge,  to  any person
# obtaining a  copy of  this software  and associated documentation
# files  (the  "Software"),  to   deal  in  the  Software   without
# restriction,  including  without limitation  the  rights to  use,
# copy, modify, merge, publish, distribute, sublicense, and/or sell
# copies  of  the  Software,  and to  permit  persons  to  whom the
# Software  is  furnished  to  do  so,  subject  to  the  following
# conditions:
#
# The above copyright  notice and this  permission notice shall  be
# included in all copies or substantial portions of the Software.
```

#
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED,
INCLUDING BUT NOT LIMITED TO THE WARRANTIES
OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY,
WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING
FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR
OTHER DEALINGS IN THE SOFTWARE.
/* --
ia64_flags.h - Copyright (c) 2000 Hewlett Packard Company

IA64/unix Foreign Function Interface

Original author: Hans Boehm, HP Labs

Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be included
in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS
FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY,
WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER
DEALINGS IN THE SOFTWARE.
-- */
pybench License

This copyright notice and license applies to all files in the pybench
directory of the pybench distribution.

Copyright (c), 1997-2006, Marc-Andre Lemburg (mal@lemburg.com)
Copyright (c), 2000-2006, eGenix.com Software GmbH (info@egenix.com)

All Rights Reserved.

Permission to use, copy, modify, and distribute this software and its
documentation for any purpose and without fee or royalty is hereby
granted, provided that the above copyright notice appear in all copies
and that both that copyright notice and this permission notice appear
in supporting documentation or portions thereof, including
modifications, that you make.

THE AUTHOR MARC-ANDRE LEMBURG DISCLAIMS ALL WARRANTIES WITH REGARD TO
THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND
FITNESS, IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL,
INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING
FROM LOSS OF USE, DATA OR PROFITS, WHETHER
IN AN ACTION OF CONTRACT,
NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION
WITH THE USE OR PERFORMANCE OF THIS SOFTWARE !
Secret Labs' Regular Expression Engine
#
re-compatible interface for the sre matching engine
#
Copyright (c) 1998-2001 by Secret Labs AB. All rights reserved.
#
This version of the SRE library can be redistributed under CNRI's
Python 1.6 license. For any other use, please contact Secret Labs
AB (info@pythonware.com).
#
Portions of this engine have been developed in cooperation with
CNRI. Hewlett-Packard provided funding for 1.6 integration and
other compatibility work.
libffi - Copyright (c) 1996-2014 Anthony Green, Red Hat, Inc and others.
See source files for details.

Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
``Software''), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED ``AS IS'', WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.
IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY
CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF

CONTRACT,
TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
Licenses and Acknowledgements for Incorporated Software
==========

This section is an incomplete, but growing list of licenses and acknowledgements
for third-party software incorporated in the Python distribution.

Mersenne Twister

The :mod:'_random' module includes code based on a download from
http://www.math.keio.ac.jp/ matumoto/MT2002/emt19937ar.html. The following are
the verbatim comments from the original code::

A C-program for MT19937, with initialization improved 2002/1/26.
Coded by Takuji Nishimura and Makoto Matsumoto.

Before using, initialize the state by using init_genrand(seed)
or init_by_array(init_key, key_length).

Copyright (C) 1997 - 2002, Makoto Matsumoto and Takuji Nishimura,
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the
following conditions
are met:

1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

3. The names of its contributors may not be used to endorse or promote
products derived from this software without specific prior written
permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY,

OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR
PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Any feedback is very welcome.
http://www.math.keio.ac.jp/matumoto/emt.html
email: matumoto@math.keio.ac.jp

Sockets

The :mod:'socket' module uses the functions, :func:'getaddrinfo', and
:func:'getnameinfo', which are coded in separate source files from the WIDE
Project, http://www.wide.ad.jp/. ::

Copyright (C) 1995, 1996, 1997, and 1998 WIDE Project.
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided
that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.
3. Neither the name of the project nor the names of its contributors
   may be used to endorse or promote products derived from this software
   without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS "AS IS" AND
GAI_ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE
FOR GAI_ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON GAI_ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN GAI_ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

Floating point exception control

The source for the :mod:'fpectl' module includes the following notice::

```
   ---------------------------------------------------------------------
  /                    Copyright (c) 1996.                        \
 |         The Regents of the University of California.             |
 |                    All rights reserved.                         |
 |
        |
 |  Permission to use, copy, modify, and distribute this software for  |
 |  any purpose without fee is hereby granted, provided that this en-  |
 |  tire notice is included in all copies of any software which is or  |
 |  includes  a  copy  or  modification  of  this software and in all  |
 |  copies of the supporting documentation for such software.          |
 |                                                                     |
 |  This  work was produced at the University of California, Lawrence  |
 |  Livermore National Laboratory under  contract  no.  W-7405-ENG-48  |
 |  between  the  U.S.  Department  of  Energy and The Regents of the  |
 |  University of California for the operation of UC LLNL.             |
 |                                                                     |
 |                         DISCLAIMER                                  |
 |
                                     |
 |  This  software was prepared as an account of work sponsored by an  |
 |  agency of the United States Government. Neither the United States  |
 |  Government  nor the University of California nor any of their em-  |
 |  ployees, makes any warranty, express or implied, or  assumes  any  |
 |  liability  or  responsibility  for the accuracy, completeness, or  |
 |  usefulness of any information,  apparatus,  product,  or  process  |
 |  disclosed,   or  represents  that  its  use  would  not  infringe  |
 |  privately-owned rights. Reference herein to any specific  commer-  |
 |  cial  products,  process,  or  service  by trade name, trademark,  |
 |  manufacturer, or otherwise, does not  necessarily  constitute  or  |
 |  imply  its endorsement, recommendation, or favoring by the United  |
 |  States Government or the University of California. The views
 and  |
 |  opinions  of authors expressed herein do not necessarily state or  |
 |  reflect those of the United States Government or  the  University  |
 |  of  California,  and shall not be used for advertising or product  |
  \ endorsement purposes.                                            /
   ---------------------------------------------------------------------
```

MD5 message digest algorithm

The source code for the :mod:'md5' module contains the following notice::

Copyright (C) 1999, 2002 Aladdin Enterprises. All rights reserved.

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

L. Peter Deutsch
ghost@aladdin.com

Independent implementation of MD5 (RFC 1321).

This code implements the MD5 Algorithm defined in RFC 1321, whose text is available at
http://www.ietf.org/rfc/rfc1321.txt
The code is derived from the text of the RFC, including the test suite (section A.5) but excluding the rest of Appendix A. It does not include

any code or documentation that is identified in the RFC as being copyrighted.

The original and principal author of md5.h is L. Peter Deutsch <ghost@aladdin.com>. Other authors are noted in the change history that follows (in reverse chronological order):

2002-04-13 lpd Removed support for non-ANSI compilers; removed references to Ghostscript; clarified derivation from RFC 1321; now handles byte order either statically or dynamically.
1999-11-04 lpd Edited comments slightly for automatic TOC extraction.
1999-10-18 lpd Fixed typo in header comment (ansi2knr rather than md5); added conditionalization for C++ compilation from Martin Purschke <purschke@bnl.gov>.

1999-05-03 lpd Original version.

Asynchronous socket services

The :mod:'asynchat' and :mod:'asyncore' modules contain the following notice::

Copyright 1996 by Sam Rushing

All Rights Reserved

Permission to use, copy, modify, and distribute this software and
its documentation for any purpose and without fee is hereby
granted, provided that the above copyright notice appear in all
copies and that both that copyright notice and this permission
notice appear in supporting documentation, and that the name of Sam
Rushing not be used in advertising or publicity pertaining to
distribution of the software without specific, written prior
permission.

SAM RUSHING DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE,
INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN
NO EVENT SHALL SAM RUSHING BE LIABLE FOR ANY SPECIAL, INDIRECT OR
CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS
OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT,
NEGLIGENCE OR OTHER TORTIOUS ACTION,
ARISING OUT OF OR IN
CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Cookie management

The :mod:'Cookie' module contains the following notice::

Copyright 2000 by Timothy O'Malley <timo@alum.mit.edu>

All Rights Reserved

Permission to use, copy, modify, and distribute this software
and its documentation for any purpose and without fee is hereby
granted, provided that the above copyright notice appear in all
copies and that both that copyright notice and this permission
notice appear in supporting documentation, and that the name of
Timothy O'Malley not be used in advertising or publicity
pertaining to distribution of the software without specific, written

prior permission.

Timothy O'Malley DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS
SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS, IN NO EVENT SHALL
Timothy O'Malley BE LIABLE FOR
ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS,
WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS
ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Profiling

The :mod:'profile' and :mod:'pstats' modules contain the following notice::

Copyright 1994, by InfoSeek Corporation, all rights reserved.
Written by James Roskind

Permission to use, copy, modify, and distribute this Python software
and its associated documentation for any purpose (subject to the
restriction in the following sentence) without fee is hereby granted,
provided that the above copyright notice appears in all copies, and
that both that copyright notice and this permission notice appear in
supporting documentation, and that the name of InfoSeek not be used
in
advertising or publicity pertaining to distribution of the software
without specific, written prior permission. This permission is
explicitly restricted to the copying and modification of the software
to remain in Python, compiled Python, or other languages (such as C)
wherein the modified or derived code is exclusively imported into a
Python module.

INFOSEEK CORPORATION DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS
SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND
FITNESS. IN NO EVENT SHALL INFOSEEK CORPORATION BE LIABLE FOR ANY
SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER
RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF
CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN
CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Execution tracing

The :mod:'trace' module contains the following

notice::

portions copyright 2001, Autonomous Zones Industries, Inc., all rights...
err... reserved and offered to the public under the terms of the
Python 2.2 license.
Author: Zooko O'Whielacronx
http://zooko.com/
mailto:zooko@zooko.com

Copyright 2000, Mojam Media, Inc., all rights reserved.
Author: Skip Montanaro

Copyright 1999, Bioreason, Inc., all rights reserved.
Author: Andrew Dalke

Copyright 1995-1997, Automatrix, Inc., all rights reserved.
Author: Skip Montanaro

Copyright 1991-1995, Stichting Mathematisch Centrum, all rights reserved.

Permission to use, copy, modify, and distribute this Python software and
its associated documentation for any purpose without fee is hereby
granted, provided that the above copyright notice appears in all copies,
and that both that copyright notice and this permission notice appear in
supporting documentation,
and that the name of neither Automatrix,
Bioreason or Mojam Media be used in advertising or publicity pertaining to
distribution of the software without specific, written prior permission.

UUencode and UUdecode functions

The :mod:'uu' module contains the following notice::

Copyright 1994 by Lance Ellinghouse
Cathedral City, California Republic, United States of America.
All Rights Reserved
Permission to use, copy, modify, and distribute this software and its
documentation for any purpose and without fee is hereby granted,
provided that the above copyright notice appear in all copies and that
both that copyright notice and this permission notice appear in
supporting documentation, and that the name of Lance Ellinghouse
not be used in advertising or publicity pertaining to distribution
of the software without specific, written prior permission.

LANCE ELLINGHOUSE DISCLAIMS ALL WARRANTIES WITH REGARD TO

THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL LANCE ELLINGHOUSE CENTRUM BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Modified by Jack Jansen, CWI, July 1995:
- Use binascii module to do the actual line-by-line conversion
  between ascii and binary. This results in a 1000-fold speedup. The C
  version is still 5 times faster, though.
- Arguments more compliant with python standard

XML Remote Procedure Calls

The :mod:'xmlrpclib' module contains the following notice::

The XML-RPC client interface is

Copyright (c) 1999-2002 by Secret Labs AB
Copyright (c) 1999-2002 by Fredrik Lundh

By obtaining, using, and/or copying this software and/or its associated documentation, you agree that you have read, understood, and will comply with the following terms and conditions:

Permission to use, copy, modify, and distribute this software and its associated documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies, and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Secret Labs AB or the author not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

SECRET LABS AB AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANT-ABILITY
AND FITNESS. IN NO EVENT SHALL SECRET LABS AB OR THE AUTHOR BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

test_epoll

The :mod:'test_epoll' contains the following notice::

Copyright (c) 2001-2006 Twisted Matrix Laboratories.

Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE
LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION
WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Select kqueue

The :mod:'select' and contains the following notice for the kqueue interface::

Copyright (c) 2000 Doug White, 2006 James Knight, 2007 Christian Heimes
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that
the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS "AS IS" AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE

ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.
* Copyright (C) 1995, 1996, 1997, and 1998 WIDE Project.
* All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the above copyright
*   notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*   notice, this list of conditions and the following disclaimer in the
*   documentation and/or other materials provided with the distribution.
* 3. Neither the name of the project nor the names of its contributors
*   may be used to endorse or promote products derived from this software
*   without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS "AS IS" AND
* GAI_ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY
 AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE
* FOR GAI_ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON GAI_ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN GAI_ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
# Copyright (c) 2001-2006 Twisted Matrix Laboratories.
#
Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:
#
The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.

#
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE
LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY,
WHETHER IN AN ACTION
OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION
WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd
and Clark Cooper
Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006 Expat maintainers.

Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be included
in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.
IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE
LIABLE FOR ANY
CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT,
TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
/* zlib.h -- interface of the 'zlib' general purpose compression library
version 1.2.3, July 18th, 2005

Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied
warranty. In no event will the authors be held liable for any damages
arising from the use of this software.

Permission is granted to anyone to use this software for any purpose,
including commercial applications, and to alter it and redistribute it
freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not
claim that you wrote the original software. If you use this software
in a product, an acknowledgment in the product documentation would be

appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org
Mark Adler madler@alumni.caltech.edu

The data format used by the zlib library is described by RFCs (Request for Comments) 1950 to 1952 in the files http://www.ietf.org/rfc/rfc1950.txt (zlib format), rfc1951.txt (deflate format) and rfc1952.txt (gzip format).
*/

Files in this directory from from Bob Ippolito's py2app.

License: Any components of the py2app suite may be distributed under the MIT or PSF open source licenses.

This is version 1.0, SVN revision 789, from 2006/01/25.
The main repository is http://svn.red-bean.com/bob/macholib/trunk/macholib/

X Window System License - X11R6.4

Copyright (c) 1998 The Open Group

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE OPEN GROUP BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE,

ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of The Open Group shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization

from The Open Group.

X Window System is a trademark of The Open Group
Copyright 2001-2004 by Vinay Sajip. All Rights Reserved.
#
Permission to use, copy, modify, and distribute this software and its
documentation for any purpose and without fee is hereby granted,
provided that the above copyright notice appear in all copies and that
both that copyright notice and this permission notice appear in
supporting documentation, and that the name of Vinay Sajip
not be used in advertising or publicity pertaining to distribution
of the software without specific, written prior permission.
VINAY SAJIP DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING
ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL
VINAY SAJIP BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR
ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER
IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT
OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Additional Conditions for this Windows binary build

This program is linked with and uses Microsoft Distributable Code,
copyrighted by Microsoft Corporation. The Microsoft Distributable Code
includes the following files:

msvcr90.dll
msvcp90.dll
msvcm90.dll

If you further distribute programs that include the Microsoft
Distributable Code, you must comply with the restrictions on
distribution specified by Microsoft. In particular, you must require
distributors and external end users to agree to terms that protect the
Microsoft Distributable Code at least as much as Microsoft's own
requirements for the Distributable Code. See Microsoft's documentation
(included in its developer tools and on its website at microsoft.com)
for specific details.

Redistribution of the Windows binary build of the Python interpreter
complies with this agreement, provided that you do not:

- alter any copyright, trademark or patent notice in Microsoft's
Distributable
 Code;

- use Microsoft's trademarks in your programs' names or in a way that

suggests your programs come from or are endorsed by Microsoft;

- distribute Microsoft's Distributable Code to run on a platform other
than Microsoft operating systems, run-time technologies or application
platforms; or

- include Microsoft Distributable Code in malicious, deceptive or
unlawful programs.

These restrictions apply only to the Microsoft Distributable Code as
defined above, not to Python itself or any programs running on the
Python interpreter. The redistribution of the Python interpreter and
libraries is governed by the Python Software License included with this
file, or by other licenses as marked.

1.16 openssh 7.3p1

1.16.1 Available under license :

This file is part of the OpenSSH software.

The licences which components of this software fall under are as
follows. First, we will summarize and say that all components
are under a BSD licence, or a licence more free than that.

OpenSSH contains no GPL code.

1)
```
 * Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland
 *                    All rights reserved
 *
 * As far as I am concerned, the code I have written for this software
 * can be used freely for any purpose.  Any derived versions of this
 * software must be clearly marked as such, and if the derived work is
 * incompatible with the protocol description in the RFC file, it must be
 * called by a name other than "ssh" or "Secure Shell".
```

[Tatu continues]
```
 *  However, I am not implying to give any licenses to any patents or
 * copyrights held by third parties, and the software includes parts that
 * are not under my direct control.  As far as I know, all included

* source code is used in accordance with the relevant license agreements
 * and can be used freely for any purpose (the GNU license being the most
 * restrictive); see below for details.
```

[However, none of that term is relevant at this point in time. All of
these restrictively licenced software components which he talks about

have been removed from OpenSSH, i.e.,

- RSA is no longer included, found in the OpenSSL library
- IDEA is no longer included, its use is deprecated
- DES is now external, in the OpenSSL library
- GMP is no longer used, and instead we call BN code from OpenSSL
- Zlib is now external, in a library
- The make-ssh-known-hosts script is no longer included
- TSS has been removed
- MD5 is now external, in the OpenSSL library
- RC4 support has been replaced with ARC4 support from OpenSSL
- Blowfish is now external, in the OpenSSL library

[The licence continues]

Note that any information and
cryptographic algorithms used in this
software are publicly available on the Internet and at any major
bookstore, scientific library, and patent office worldwide. More
information can be found e.g. at "http://www.cs.hut.fi/crypto".

The legal status of this program is some combination of all these
permissions and restrictions. Use only at your own responsibility.
You will be responsible for any legal consequences yourself; I am not
making any claims whether possessing or using this is legal or not in
your country, and I am not taking any responsibility on your behalf.

NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY
FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES
PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED
OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS
TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE
PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING,
REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING
WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR
REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES,
INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING
OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED
TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY
YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER

PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

2)
The 32-bit CRC compensation attack detector in deattack.c was contributed by
CORE SDI S.A. under a BSD-style license.

```
 * Cryptographic attack detector for ssh - source code
 *
 * Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina.
 *
 * All rights reserved. Redistribution and use in source and binary
 * forms, with or without modification, are permitted provided that
 * this copyright notice is retained.
 *
 * THIS SOFTWARE IS PROVIDED ``AS IS" AND ANY EXPRESS OR IMPLIED
 * WARRANTIES ARE DISCLAIMED. IN NO EVENT SHALL CORE SDI S.A. BE
 * LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR
 * CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OR MISUSE OF THIS
 * SOFTWARE.
 *
 * Ariel Futoransky <futo@core-sdi.com>
 * <http://www.core-sdi.com>
```

3)
ssh-keyscan was contributed by David Mazieres under a BSD-style license.

```
 * Copyright 1995, 1996 by David Mazieres <dm@lcs.mit.edu>.
 *
 * Modification and redistribution in source and binary forms is
 * permitted
provided that due credit is given to the author and the
 * OpenBSD project by leaving this copyright notice intact.
```

4)
The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers and Paulo Barreto is in the public domain and distributed with the following license:

```
 * @version 3.0 (December 2000)
 *
 * Optimised ANSI C code for the Rijndael cipher (now AES)
 *
 * @author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>
 * @author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be>
 * @author Paulo Barreto <paulo.barreto@terra.com.br>
```

```
 *
 * This code is hereby placed in the public domain.
 *
 * THIS SOFTWARE IS PROVIDED BY THE AUTHORS "AS IS" AND ANY EXPRESS
 * OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
 * WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE
 * LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY, OR
 * CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
 * SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
 * BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
 * WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE
 * OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE,
 * EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

5)

One component of the ssh source code is under a 3-clause BSD license, held by the University of California, since we pulled these parts from original Berkeley code.

```
 * Copyright (c) 1983, 1990, 1992, 1993, 1995
 *      The Regents of the University of California.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain
the above copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. Neither the name of the University nor the names of its contributors
 *    may be used to endorse or promote products derived from this software
 *    without specific prior written permission.
 *
 * THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS" AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT
OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
```

* SUCH DAMAGE.

6)

Remaining components of the software are provided under a standard
2-term BSD licence with the following names as copyright holders:

Markus Friedl
Theo de Raadt
Niels Provos
Dug Song
Aaron Campbell
Damien Miller
Kevin Steves
Daniel Kouril
Wesley Griffin
Per Allansson
Nils Nordman
Simon Wilkinson

Portable OpenSSH additionally includes code from the following copyright
holders, also under the 2-term BSD license:

Ben Lindstrom
Tim Rice
Andre Lucas
Chris Adams
Corinna Vinschen
Cray Inc.
Denis Parker
Gert Doering
Jakob Schlyter
Jason Downs
Juha Yrjl
Michael Stone
Networks Associates Technology,
Inc.
Solar Designer
Todd C. Miller
Wayne Schroeder
William Jones
Darren Tucker
Sun Microsystems
The SCO Group
Daniel Walsh
Red Hat, Inc
Simon Vallet / Genoscope

* Redistribution and use in source and binary forms, with or without

```
   * modification, are permitted provided that the following conditions
   * are met:
   * 1. Redistributions of source code must retain the above copyright
   *    notice, this list of conditions and the following disclaimer.
   * 2. Redistributions in binary form must reproduce the above copyright
   *    notice, this list of conditions and the following disclaimer in the
   *    documentation and/or other materials provided with the distribution.
   *
   * THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR
   * IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
   * OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
   * IN NO EVENT SHALL THE AUTHOR
BE LIABLE FOR ANY DIRECT, INDIRECT,
   * INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
   * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
   * DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
   * THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
   * (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF
   * THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

8) Portable OpenSSH contains the following additional licenses:

a) md5crypt.c, md5crypt.h

```
 * "THE BEER-WARE LICENSE" (Revision 42):
 * <phk@login.dknet.dk> wrote this file.  As long as you retain this
 * notice you can do whatever you want with this stuff. If we meet
 * some day, and you think this stuff is worth it, you can buy me a
 * beer in return.   Poul-Henning Kamp
```

b) snprintf replacement

```
* Copyright Patrick Powell 1995
* This code is based on code written by Patrick
Powell
* (papowell@astart.com) It may be used for any purpose as long as this
* notice remains intact on all source code distributions
```

c) Compatibility code (openbsd-compat)

Apart from the previously mentioned licenses, various pieces of code in the openbsd-compat/ subdirectory are licensed as follows:

Some code is licensed under a 3-term BSD license, to the following copyright holders:

Todd C. Miller
Theo de Raadt

Damien Miller
Eric P. Allman
The Regents of the University of California
Constantin S. Svintsoff

* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the above copyright
*   notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*   notice, this list of conditions and the following disclaimer in the
*
  documentation and/or other materials provided with the distribution.
* 3. Neither the name of the University nor the names of its contributors
*   may be used to endorse or promote products derived from this software
*   without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN
IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.

Some code is licensed under an ISC-style license, to the following
copyright holders:

Internet Software Consortium.
Todd C. Miller
Reyk Floeter
Chad Mynhier

* Permission to use, copy, modify, and distribute this software for any
* purpose with or without fee is hereby granted, provided that the above
* copyright notice and this permission notice appear in all copies.
*
* THE SOFTWARE IS PROVIDED "AS IS" AND TODD C. MILLER DISCLAIMS ALL
* WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES
* OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL TODD C. MILLER BE LIABLE
* FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
* WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION

* OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN
* CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Some code is licensed under
a MIT-style license to the following
copyright holders:

Free Software Foundation, Inc.

* Permission is hereby granted, free of charge, to any person obtaining a *
* copy of this software and associated documentation files (the *
* "Software"), to deal in the Software without restriction, including *
* without limitation the rights to use, copy, modify, merge, publish, *
* distribute, distribute with modifications, sublicense, and/or sell *
* copies of the Software, and to permit persons to whom the Software is *
* furnished to do so, subject to the following conditions: *
* *
* The above copyright notice and this permission notice shall be included *
* in all copies or substantial portions of the Software. *
* *
* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT
WARRANTY OF ANY KIND, EXPRESS *
* OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF *
* MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. *
* IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, *
* DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR *
* OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR *
* THE USE OR OTHER DEALINGS IN THE SOFTWARE. *
* *
* Except as contained in this notice, the name(s) of the above copyright *
* holders shall not be used in advertising or otherwise to promote the *
* sale, use or other dealings in this Software without prior written *
* authorization. *
**********/

$OpenBSD: LICENCE,v 1.19
2004/08/30 09:18:08 markus Exp $

1.17 gnutls 3.5.3

1.17.1 Available under license :

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts
as the successor of the GNU Library Public License, version 2, hence
the version number 2.1.]

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
Licenses are intended to guarantee your freedom to share and change
free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some
specially designated software packages--typically libraries--of the
Free Software Foundation and other authors who decide to use it. You
can use it too, but we suggest
you first think carefully about whether
this license or the ordinary General Public License is the better
strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use,
not price. Our General Public Licenses are designed to make sure that
you have the freedom to distribute copies of free software (and charge
for this service if you wish); that you receive source code or can get
it if you want it; that you can change the software and use pieces of
it in new free programs; and that you are informed that you can do
these things.

To protect your rights, we need to make restrictions that forbid
distributors to deny you these rights or to ask you to surrender these
rights. These restrictions translate to certain responsibilities for
you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis
or for a fee, you must give the recipients
all the rights that we gave
you. You must make sure that they, too, receive or can get the source
code. If you link other code with the library, you must provide
complete object files to the recipients, so that they can relink them
with the library after making changes to the library and recompiling
it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the
library, and (2) we offer you this license, which gives you legal
permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use

the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without
limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square

root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves,
then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to
a given copy of the Library. To do
this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed
under the terms of Sections 1 and 2 above on a
medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License.
Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the

Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on

which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further

restrictions on the recipients' exercise of the rights granted herein.
You are not responsible for enforcing compliance by third parties with
this License.

11. If, as a consequence of a court judgment or allegation of patent
infringement or for any other reason (not limited to patent issues),
conditions are imposed on you (whether by court order, agreement or
otherwise) that contradict the conditions of this License, they do not
excuse you from the conditions of this License. If you cannot
distribute
so as to satisfy simultaneously your obligations under this
License and any other pertinent obligations, then as a consequence you
may not distribute the Library at all. For example, if a patent
license would not permit royalty-free redistribution of the Library by
all those who receive copies directly or indirectly through you, then
the only way you could satisfy both it and this License would be to
refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any
particular circumstance, the balance of the section is intended to apply,
and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any
patents or other property right claims or to contest validity of any
such claims; this section has the sole purpose of protecting the
integrity of the free software distribution system which is
implemented by public license practices. Many people
have made
generous contributions to the wide range of software distributed
through that system in reliance on consistent application of that
system; it is up to the author/donor to decide if he or she is willing
to distribute software through any other system and a licensee cannot
impose that choice.

This section is intended to make thoroughly clear what is believed to
be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in
certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Library under this License may add
an explicit geographical distribution limitation excluding those countries,
so that distribution is permitted only in or among countries not thus
excluded. In such case, this License incorporates the limitation as if
written in the body of this License.

13. The Free Software Foundation may publish revised and/or new
versions of the Lesser General Public

License from time to time.
Such new versions will be similar in spirit to the present version,
but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library
specifies a version number of this License which applies to it and
"any later version", you have the option of following the terms and
conditions either of that version or of any later version published by
the Free Software Foundation. If the Library does not specify a
license version number, you may choose any version ever published by
the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free
programs whose distribution conditions are incompatible with these,
write to the author to ask for permission. For software which is
copyrighted by the Free Software Foundation, write to the Free
Software Foundation; we sometimes make exceptions for this. Our
decision will be guided by the two goals of preserving the free status
of
all derivatives of our free software and of promoting the sharing
and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO
WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW.
EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR
OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY
KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE
LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME
THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN
WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY
AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU
FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR
CONSEQUENTIAL
DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE
LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING
RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A
FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF
SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH
DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line
and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or
modify it under the terms of the GNU Lesser General Public
License as published by the Free Software Foundation; either
version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public
License along with this library; if not, write to the Free Software
Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should
also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the library, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the
library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!
Statement of Purpose

The laws of most jurisdictions throughout the world automatically confer exclusive Copyright and Related Rights

(defined below) upon the creator and subsequent owner(s) (each and all, an "owner") of an original work of authorship and/or a database (each, a "Work").

Certain owners wish to permanently relinquish those rights to a Work for the purpose of contributing to a commons of creative, cultural and scientific works ("Commons") that the public can reliably and without fear of later claims of infringement build upon, modify, incorporate in other works, reuse and redistribute as freely as possible in any form whatsoever and for any purposes, including without limitation commercial purposes. These owners may contribute to the Commons to promote the ideal of a free culture and the further production of creative, cultural and scientific works, or to gain reputation or greater distribution for their Work in part through the use and efforts of others.

For these and/or
other purposes and motivations, and without any expectation of additional consideration or compensation, the person associating CC0 with a Work (the "Affirmer"), to the extent that he or she is an owner of Copyright and Related Rights in the Work, voluntarily elects to apply CC0 to the Work and publicly distribute the Work under its terms, with knowledge of his or her Copyright and Related Rights in the Work and the meaning and intended legal effect of CC0 on those rights.

1. Copyright and Related Rights. A Work made available under CC0 may be protected by copyright and related or neighboring rights ("Copyright and Related Rights"). Copyright and Related Rights include, but are not limited to, the following:

the right to reproduce, adapt, distribute, perform, display, communicate, and translate a Work;
moral rights retained by the original author(s) and/or performer(s);
publicity and privacy rights pertaining to a person's image or likeness depicted in a Work;
rights
protecting against unfair competition in regards to a Work, subject to the limitations in paragraph 4(a), below;
rights protecting the extraction, dissemination, use and reuse of data in a Work;
database rights (such as those arising under Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, and under any national implementation thereof, including any amended or successor version of such directive); and
other similar, equivalent or corresponding rights throughout the world based on applicable law or treaty, and any national implementations thereof.

2. Waiver. To the greatest extent permitted by, but not in contravention of, applicable law, Affirmer hereby overtly, fully, permanently, irrevocably and unconditionally waives, abandons, and surrenders all of Affirmer's Copyright and Related Rights and associated claims and causes of action, whether now known or unknown (including existing as well as future claims
and causes of action), in the Work (i) in all territories worldwide, (ii) for the maximum duration provided by applicable law or treaty (including future time extensions), (iii) in any current or future medium and for any number of copies, and (iv) for any purpose whatsoever, including without limitation commercial, advertising or promotional purposes (the "Waiver"). Affirmer makes the Waiver for the benefit of each member of the public at large and to the detriment of Affirmer's heirs and successors, fully intending that such Waiver shall not be subject to revocation, rescission, cancellation, termination, or any other legal or equitable action to disrupt the quiet enjoyment of the Work by the public as contemplated by Affirmer's express Statement of Purpose.

3. Public License Fallback. Should any part of the Waiver for any reason be judged legally invalid or ineffective under applicable law, then the Waiver shall be preserved to the maximum extent permitted taking into account Affirmer's

express Statement of Purpose. In addition, to the extent the Waiver is so judged Affirmer hereby grants to each affected person a royalty-free, non transferable, non sublicensable, non exclusive, irrevocable and unconditional license to exercise Affirmer's Copyright and Related Rights in the Work (i) in all territories worldwide, (ii) for the maximum duration provided by applicable law or treaty (including future time extensions), (iii) in any current or future medium and for any number of copies, and (iv) for any purpose whatsoever, including without limitation commercial, advertising or promotional purposes (the "License"). The License shall be deemed effective as of the date CC0 was applied by Affirmer to the Work. Should any part of the License for any reason be judged legally invalid or ineffective under applicable law, such partial invalidity or ineffectiveness shall not invalidate the remainder of the License, and in such case Affirmer hereby affirms that he or she will
not (i) exercise any of his or her remaining Copyright and Related Rights in the Work or (ii) assert any associated claims and causes of action with respect to the Work, in either case contrary to Affirmer's express Statement of Purpose.

4. Limitations and Disclaimers.

No trademark or patent rights held by Affirmer are waived, abandoned, surrendered, licensed or otherwise affected by this document.

Affirmer offers the Work as-is and makes no representations or warranties of any kind concerning the Work, express, implied, statutory or otherwise, including without limitation warranties of title, merchantability, fitness for a particular purpose, non infringement, or the absence of latent or other defects, accuracy, or the present or absence of errors, whether or not discoverable, all to the greatest extent permissible under applicable law.

Affirmer disclaims responsibility for clearing rights of other persons that may apply to the Work or any use thereof, including without
limitation any person's Copyright and Related Rights in the Work. Further, Affirmer disclaims responsibility for obtaining any necessary consents, permissions or other rights required for any use of the Work.

Affirmer understands and acknowledges that Creative Commons is not a party to this document and has no duty or obligation with respect to this CC0 or use of the Work.

LICENSING
=========

Since GnuTLS version 3.1.10, the core library is released under
the GNU Lesser General Public License (LGPL) version 2.1 or later
(see doc/COPYING.LESSER for the license terms).

The GNU LGPL applies to the main GnuTLS library, while the
included applications as well as gnutls-openssl
library are under the GNU GPL version 3. The gnutls library is
located in the lib/ and libdane/ directories, while the applications
in src/ and, the gnutls-openssl library is at extra/.

The documentation in doc/ is under the GNU FDL license 1.3.

Note, however, that the nettle and the gmp libraries which are
GnuTLS dependencies, they are distributed under a LGPLv3+ or GPLv2+ dual
license. As such binaries linking to them need to adhere to either LGPLv3+
or the GPLv2+ license.

For any copyright year range specified as YYYY-ZZZZ in this package
note that the range specifies every single year in that closed interval.
==========
Written by Andy Polyakov <appro@fy.chalmers.se> for the OpenSSL
project. The module is, however, dual licensed under OpenSSL and
CRYPTOGAMS licenses depending on where you obtain it. For further
details see http://www.openssl.org/~appro/cryptogams/.
==========

Copyright (c) 2006-2012, CRYPTOGAMS by <appro@openssl.org>
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

* Redistributions of source code must retain copyright notices,
this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above
copyright notice, this list of conditions and the following
disclaimer in the documentation and/or other materials
provided with the distribution.

* Neither the name of the CRYPTOGAMS nor
the names of its
copyright holder and contributors may be used to endorse or
promote products derived from this software without specific
prior written permission.

ALTERNATIVELY, provided that this notice is retained in full, this
product may be distributed under the terms of the GNU General Public
License (GPL), in which case the provisions of the GPL apply INSTEAD OF
those given above.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER AND CONTRIBUTORS
"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT
OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,
OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

```
########################################################################
## Constant-time SSSE3 AES core implementation.
## version 0.1
##
## By Mike Hamburg (Stanford University), 2009
## Public domain.
##
## For details see http://shiftleft.org/papers/vector_aes/ and
## http://crypto.stanford.edu/vpaes/.
```

GNU LESSER GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 1992-2015 by Bruce Korb - all rights reserved
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and the "GNU GPL" refers to version 3 of the GNU General Public License.

"The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An "Application" is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The "Corresponding Application Code" for a Combined Work means the

object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse

engineering for debugging such modifications, if you also do each of the following:

a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

Copyright (C) 1992-2015 by Bruce Korb - all rights reserved

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided

with the distribution.

3. The name of the author may not be used to endorse or promote
products derived from this software without specific prior
written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to
freedom, not
price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you

these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1)
assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand
ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The
"System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally
available free
programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered
by this License only if the output, given its
content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose

of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed;
section 10
makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately
publish on each copy an appropriate copyright notice;
keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a

written offer, valid for at least three years
and valid for as
long as you offer spare parts or customer support for that product
model, to give anyone who possesses the object code either (1) a
copy of the Corresponding Source for all the software in the
product that is covered by this License, on a durable physical
medium customarily used for software interchange, for a price no
more than your reasonable cost of physically performing this
conveying of source, or (2) access to copy the
Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the
written offer to provide the Corresponding Source. This
alternative is allowed only occasionally and noncommercially, and
only if you received the object code with such an offer, in accord
with subsection 6b.

d) Convey the object code by offering access from a designated
place (gratis or for a charge), and offer equivalent access to the
Corresponding Source in
the same way through the same place at no
further charge. You need not require recipients to copy the
Corresponding Source along with the object code. If the place to
copy the object code is a network server, the Corresponding Source
may be on a different server (operated by you or a third party)
that supports equivalent copying facilities, provided you maintain
clear directions next to the object code saying where to find the
Corresponding Source. Regardless of what server hosts the
Corresponding Source, you remain obligated to ensure that it is
available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided
you inform other peers where the object code and Corresponding
Source of the work are being offered to the general public at no
charge under subsection 6d.

A separable portion of the object code, whose source code is excluded
from the Corresponding Source
as a System Library, need not be
included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any
tangible personal property which is normally used for personal, family,
or household purposes, or (2) anything designed or sold for incorporation
into a dwelling. In determining whether a product is a consumer product,
doubtful cases shall be resolved in favor of coverage. For a particular
product received by a particular user, "normally used" refers to a
typical or common use of that class of product, regardless of the status

of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent

that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or
limiting liability differently from the
terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on

those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms

of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above
requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright
holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However,

nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights
granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For
purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily

for and in connection with specific products or compilations that
contain the covered work, unless you entered into that arrangement,
or
that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting
any implied license or other defenses to infringement that may
otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or
otherwise) that contradict the conditions of this License, they do not
excuse you from the conditions of this License. If you cannot convey a
covered work so as to satisfy simultaneously your obligations under this
License and any other pertinent obligations, then as a consequence you may
not convey it at all. For example, if you agree to terms that obligate you
to collect a royalty for further conveying from those to whom you convey
the Program, the only way you could satisfy both those terms and this
License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have
permission to link or combine any covered work with a work licensed
under version 3 of the GNU Affero General Public License into a single
combined work, and to convey the resulting work. The terms of this
License will continue to apply to the part which is the covered work,
but the special requirements of the GNU Affero General Public License,
section 13, concerning interaction through a network will apply to the
combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of
the GNU General Public License from time to time. Such new versions will
be similar in spirit to the present version, but may differ in detail to
address new problems or concerns.

Each version is given a distinguishing version number. If the
Program specifies that a certain numbered version of the GNU General
Public License "or any later version" applies to it, you
have the
option of following the terms and conditions either of that numbered
version or of any later version published by the Free Software
Foundation. If the Program does not specify a version number of the
GNU General Public License, you may choose any version ever published
by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY
OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17.
Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest
possible use to the public, the best way to achieve this is to make it
free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest
to attach them to the start of each source file to most effectively
state the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where
the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation, either version 3 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>
This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program

into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what you want to
 do, use the GNU Lesser General
Public License instead of this License. But first, please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.
The MIT License (MIT)

Copyright (c) 2016 Wrymouth Innovation Ltd

Permission is hereby granted, free of charge, to any person obtaining a
copy of this software and associated documentation files (the "Software"),
to deal in the Software without restriction, including without limitation
the rights to use, copy, modify, merge, publish, distribute, sublicense,
and/or sell copies of the Software, and to permit persons to whom the
Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included
in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL
THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR
OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE,
ARISING FROM,
 OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR
OTHER DEALINGS IN THE SOFTWARE.
                GNU GENERAL PUBLIC LICENSE
                 Version 3, 29 June 2007

Copyright (C) 1992-2015 by Bruce Korb - all rights reserved
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

                      Preamble

 The GNU General Public License is a free, copyleft license for
software and other kinds of works.

 The licenses for most software and other practical works are designed
to take away your freedom to share and change the works. By contrast,
the GNU General Public License is intended to guarantee your freedom to
share and change all versions of a program--to make sure it remains free
software for all its users. We, the Free Software Foundation, use the
GNU General Public License for most of our software; it applies also to
any other work released this way by its authors. You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom,
not
price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps:
(1) assert
copyright on the software, and (2) offer you this License
giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we
stand ready
to extend this provision to those domains in future versions
of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that

patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients"
may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited

permission to run the unmodified Program. The output from running a covered work is covered by
this License only if the output, given its
content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section
10
makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish
on each copy an appropriate copyright notice;
keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization
keys, or other information required to install
and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic
Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted
or affirmed under this License. For example, you may
not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted

by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered

work if you are a party to an arrangement with a third party that is
in the business of distributing software, under which you make payment
to the third party based on the extent of your activity of conveying
the work, and under which the third party grants, to any of the
parties who would receive the covered work from you, a discriminatory
patent license (a) in connection with copies of the covered work
conveyed by you (or copies made from those copies), or (b) primarily
for and in connection with specific products or compilations that
contain the covered work, unless you entered into that arrangement,
or
that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting
any implied license or other defenses to infringement that may
otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or
otherwise) that contradict the conditions of this License, they do not
excuse you from the conditions of this License. If you cannot convey a
covered work so as to satisfy simultaneously your obligations under this
License and any other pertinent obligations, then as a consequence you may
not convey it at all. For example, if you agree to terms that obligate you
to collect a royalty for further conveying from those to whom you convey
the Program, the only way you could satisfy both those terms and this
License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have
permission to link or combine any covered work with a work licensed
under version 3 of the GNU Affero General Public License into a single
combined work, and to convey the resulting work. The terms of this
License will continue to apply to the part which is the covered work,
but the special requirements of the GNU Affero General Public License,
section 13, concerning interaction through a network will apply to the
combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of
the GNU General Public License from time to time. Such new versions will
be similar in spirit to the present version, but may differ in detail to
address new problems or concerns.

Each version is given a distinguishing version number. If the
Program specifies that a certain numbered version of the GNU General

Public License "or any later version" applies to it, you have the option
of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY
OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation
of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates

an absolute waiver of all civil liability in connection with the
Program, unless a warranty or assumption of liability accompanies a
copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest
possible use to the public, the best way to achieve this is to make it
free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest
to attach them to the start of each source file to most effectively
state the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where the full
notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) by Bruce Korb - all rights reserved

This program is free software: you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation, either version 3 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

<program> Copyright (C) by Bruce Korb - all rights reserved
This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what
you want to do, use the GNU Lesser General
Public License instead of this License. But first, please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.

1.18 libarchive 3.2.2

1.18.1 Available under license :

The libarchive distribution as a whole is Copyright by Tim Kientzle
and is subject to the copyright notice reproduced at the bottom of
this file.

Each individual file in this distribution should have a clear
copyright/licensing statement at the beginning of the file. If any do
not, please let me know and I will rectify it. The following is
intended to summarize the copyright status of the individual files;
the actual statements in the files are controlling.

* Except as listed below, all C sources (including .c and .h files)
 and documentation files are subject to the copyright notice reproduced
 at the bottom of this file.

* The following source files are also subject in whole or in part to
 a 3-clause UC Regents copyright; please read the individual source
 files for details:
  libarchive/archive_entry.c
  libarchive/archive_read_support_filter_compress.c
  libarchive/archive_write_add_filter_compress.c
  libarchive/mtree.5

* The following source files are in the public domain:
   libarchive/archive_getdate.c

* The build files---including Makefiles, configure scripts,
 and auxiliary scripts used as part of the compile process---have
 widely varying licensing terms. Please check individual files before
 distributing them to see if those restrictions apply to you.

I intend for all new source code to use the license below and hope over

time to replace code with other licenses with new implementations that
do use the license below. The varying licensing of the build scripts
seems to be an unavoidable mess.

Copyright (c) 2003-2009 <author(s)>
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
  notice, this list of conditions and the following disclaimer
  in this position and unchanged.
2. Redistributions in binary form must reproduce the above copyright
  notice, this
 list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR(S) ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR(S) BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

1.19 libpng 1.6.24

1.19.1 Available under license :

Copyright (c) 1998-2008 Greg Roelofs. All rights reserved.

This software is provided "as is," without warranty of any kind,
express or implied. In no event shall the author or contributors
be held liable for any damages arising in any way from the use of
this software.

The contents of this file are DUAL-LICENSED. You may modify and/or
redistribute this software according to the terms of one of the
following two licenses (at your option):

LICENSE 1 ("BSD-like with advertising clause"):

Permission is granted to anyone to use this software for any purpose,
including commercial applications, and to alter it and redistribute
it freely, subject to the following restrictions:

1. Redistributions of source code must retain the above copyright
notice, disclaimer, and this list of conditions.
2. Redistributions in binary
form must reproduce the above copyright
notice, disclaimer, and this list of conditions in the documenta-
tion and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this
software must display the following acknowledgment:

This product includes software developed by Greg Roelofs
and contributors for the book, "PNG: The Definitive Guide,"
published by O'Reilly and Associates.

LICENSE 2 (GNU GPL v2 or later):

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation; either version 2 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR
PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software Foundation,
Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

This copy of the libpng notices is provided for your convenience. In case of
any discrepancy between this copy and the notices in the file png.h that is
included in the libpng distribution, the latter shall prevail.

COPYRIGHT NOTICE, DISCLAIMER, and LICENSE:

If you modify libpng you may insert additional notices immediately following
this sentence.

This code is released under the libpng license.

libpng versions 1.0.7, July 1, 2000 through 1.6.24, August 4, 2016 are
Copyright (c) 2000-2002, 2004, 2006-2016 Glenn Randers-Pehrson, are
derived from libpng-1.0.6, and are distributed according to the same
disclaimer and license as libpng-1.0.6 with the following individuals
added to the list of Contributing Authors:

Simon-Pierre Cadieux
Eric S. Raymond
Mans Rullgard
Cosmin Truta
Gilles Vollant
James Yu

and with the following additions to the disclaimer:

There is no warranty against interference with your enjoyment of the
library or against infringement. There
is no warranty that our
efforts or the library will fulfill any of your particular purposes
or needs. This library is provided with all faults, and the entire
risk of satisfactory quality, performance, accuracy, and effort is with
the user.

Some files in the "contrib" directory and some configure-generated
files that are distributed with libpng have other copyright owners and
are released under other open source licenses.

libpng versions 0.97, January 1998, through 1.0.6, March 20, 2000, are
Copyright (c) 1998-2000 Glenn Randers-Pehrson, are derived from
libpng-0.96, and are distributed according to the same disclaimer and
license as libpng-0.96, with the following individuals added to the list
of Contributing Authors:

Tom Lane
Glenn Randers-Pehrson
Willem van Schaik

libpng versions 0.89, June 1996, through 0.96, May 1997, are
Copyright (c) 1996-1997 Andreas Dilger, are derived from libpng-0.88,
and are distributed according to the same disclaimer and license
as
libpng-0.88, with the following individuals added to the list of
Contributing Authors:

John Bowler
Kevin Bracey

Sam Bushell
Magnus Holmgren
Greg Roelofs
Tom Tanner

Some files in the "scripts" directory have other copyright owners
but are released under this license.

libpng versions 0.5, May 1995, through 0.88, January 1996, are
Copyright (c) 1995-1996 Guy Eric Schalnat, Group 42, Inc.

For the purposes of this copyright and license, "Contributing Authors"
is defined as the following set of individuals:

Andreas Dilger
Dave Martindale
Guy Eric Schalnat
Paul Schmidt
Tim Wegner

The PNG Reference Library is supplied "AS IS". The Contributing Authors
and Group 42, Inc. disclaim all warranties, expressed or implied,
including, without limitation, the warranties of merchantability and of
fitness for any purpose. The Contributing Authors and Group 42, Inc.
assume no liability for direct, indirect, incidental, special, exemplary,
or consequential damages,
which may result from the use of the PNG
Reference Library, even if advised of the possibility of such damage.

Permission is hereby granted to use, copy, modify, and distribute this
source code, or portions hereof, for any purpose, without fee, subject
to the following restrictions:

1. The origin of this source code must not be misrepresented.

2. Altered versions must be plainly marked as such and must not
be misrepresented as being the original source.

3. This Copyright notice may not be removed or altered from any
source or altered source distribution.

The Contributing Authors and Group 42, Inc. specifically permit, without
fee, and encourage the use of this source code as a component to
supporting the PNG file format in commercial products. If you use this
source code in a product, acknowledgment is not required but would be
appreciated.

END OF COPYRIGHT NOTICE, DISCLAIMER, and LICENSE.

TRADEMARK:

The name "libpng" has not been registered by the Copyright
owner
as a trademark in any jurisdiction. However, because libpng has
been distributed and maintained world-wide, continually since 1995,
the Copyright owner claims "common-law trademark protection" in any
jurisdiction where common-law trademark is recognized.

OSI CERTIFICATION:

Libpng is OSI Certified Open Source Software. OSI Certified Open Source is
a certification mark of the Open Source Initiative. OSI has not addressed
the additional disclaimers inserted at version 1.0.7.

EXPORT CONTROL:

The Copyright owner believes that the Export Control Classification
Number (ECCN) for libpng is EAR99, which means not subject to export
controls or International Traffic in Arms Regulations (ITAR) because
it is open source, publicly available software, that does not contain
any encryption software. See the EAR, paragraphs 734.3(b)(3) and
734.7(b).

Glenn Randers-Pehrson
glennrp at users.sourceforge.net
August 4, 2016

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it. (Some other Free Software Foundation software is covered by
the GNU Library General Public License instead.) You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not price.

Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which
gives you legal permission to copy,
distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law:

that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work
are not derived from the Program,
and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution
and only if you
received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to

control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source
code, even though third parties are not
compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing
or modifying
the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For

example, if a patent
license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor
to decide if he or she is willing
to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing
version number. If the Program
specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify
it under the terms of the
GNU General Public License as published by
the Free Software Foundation; either version 2 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute
it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this is
what you want to do, use the GNU Library General
Public License instead of this License.

1.20 m4 1.4.17

1.20.1 Available under license :

The files in this directory provide example uses of GNU M4.
The following copyright notice applies to each of these
description files.

Copyright (C) 2006, 2010-2012 Free Software Foundation, Inc.
This file is free software; the Free Software Foundation
gives unlimited permission to copy and/or distribute it,
with or without modifications, as long as this notice is preserved.

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for
software and other kinds of works.

The licenses for most software and other practical works are designed
to take away your freedom to share and change the works. By contrast,
the GNU General Public License is intended to guarantee your freedom to
share and change all versions of a program--to make sure it remains free
software for all its users. We, the Free Software Foundation, use the
GNU General Public License for most of our software; it applies also to
any other work released this way by its authors. You can apply it to
your programs, too.

When we speak of free software, we are referring to
freedom, not
price. Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
them if you wish), that you receive source code or can get it if you
want it, that you can change the software or use pieces of it in new
free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you
these rights or asking you to surrender the rights. Therefore, you have
certain responsibilities if you distribute copies of the software, or if
you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether

gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this

License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major

Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction

and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is

released under this License and any conditions added under section
7. This requirement modifies the requirement in section
4 to
"keep intact all notices".

c) You must license the entire work, as a whole, under this
License to anyone who comes into possession of a copy. This
License will therefore apply, along with any applicable section 7
additional terms, to the whole of the work, and all its parts,
regardless of how they are packaged. This License gives no
permission to license the work in any other way, but it does not
invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display
Appropriate Legal Notices; however, if the Program has interactive
interfaces that do not display Appropriate Legal Notices, your
work need not make them do so.

A compilation of a covered work with other separate and independent
works, which are not by their nature extensions of the covered work,
and which are not combined with it such as to form a larger program,
in or on a volume of a storage or distribution
medium, is called an
"aggregate" if the compilation and its resulting copyright are not
used to limit the access or legal rights of the compilation's users
beyond what the individual works permit. Inclusion of a covered work
in an aggregate does not cause this License to apply to the other
parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms
of sections 4 and 5, provided that you also convey the
machine-readable Corresponding Source under the terms of this License,
in one of these ways:

a) Convey the object code in, or embodied in, a physical product
(including a physical distribution medium), accompanied by the
Corresponding Source fixed on a durable physical medium
customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product
(including a physical distribution medium), accompanied by a
written offer, valid for at least three years
and valid for as
long as you offer spare parts or customer support for that product
model, to give anyone who possesses the object code either (1) a
copy of the Corresponding Source for all the software in the

product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the

additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights
granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For
purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY
OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17.
Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest
to attach them to the start of each source file to most effectively
state the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where
the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation, either version 3 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>
This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what you want to
do, use the GNU Lesser General
Public License instead of this License. But first, please read

<http://www.gnu.org/philosophy/why-not-lgpl.html>.

1.21 dropbear 2016.74

1.21.1 Available under license :

LibTomCrypt is public domain. As should all quality software be.

Tom St Denis
LibTomMath is hereby released into the Public Domain.

-- Tom St Denis
This package was debianized by Grahame Bowland <grahame.angrygoats.net> on
Tue, 17 Jun 2003 15:04:47 +0800, maintained temporarily by Matt Johnston
<matt@ucc.asn.au>, and was adopted by Gerrit Pape <pape@smarden.org> on
Sun, 16 May 2004 14:38:33 +0000.

It was downloaded from http://matt.ucc.asn.au/dropbear/

Upstream Author: Matt Johnston <matt@ucc.asn.au>

Copyright:
Dropbear contains a number of components from different sources, hence there
are a few licenses and authors involved. All licenses are fairly
non-restrictive.

The majority of code is written by Matt Johnston, under the license below.

Portions of the client-mode work are (c) 2004 Mihnea Stoenescu, under the
same license:

Copyright (c) 2002-2015 Matt Johnston
Portions copyright (c) 2004 Mihnea Stoenescu
All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all
copies or substantial portions of the Software.

THE SOFTWARE

IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

=====

LibTomCrypt and LibTomMath are written by Tom St Denis, and are Public Domain.

=====

sshpty.c is taken from OpenSSH 3.5p1,
Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland
All rights reserved
"As far as I am concerned, the code I have written for this software
can be used freely for any purpose. Any derived versions of this
software must be clearly marked as such, and if the derived work is
incompatible with the protocol description in the RFC file, it must be
called by a name other
than "ssh" or "Secure Shell". "

=====

loginrec.c
loginrec.h
atomicio.h
atomicio.c
and strlcat() (included in util.c) are from OpenSSH 3.6.1p2, and are licensed under the 2 point BSD license.

loginrec is written primarily by Andre Lucas, atomicio.c by Theo de Raadt.

strlcat() is (c) Todd C. Miller

=====

Import code in keyimport.c is modified from PuTTY's import.c, licensed as follows:

PuTTY is copyright 1997-2003 Simon Tatham.

Portions copyright Robert de Bath, Joris van Rantwijk, Delian
Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry,
Justin Bradford, and CORE SDI S.A.

Permission is hereby granted, free of charge, to any person
obtaining a copy of this software and associated documentation files
(the "Software"), to deal in the Software without restriction,
including without limitation the rights to use, copy, modify, merge,
publish, distribute, sublicense, and/or sell copies of the Software,
and to permit persons to whom the Software is furnished to do so,
subject
 to the following conditions:

The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS BE LIABLE
FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF
CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION
WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

=====

curve25519-donna:

/* Copyright 2008, Google Inc.
* All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions are
* met:
*
*   * Redistributions of source code must retain the above copyright
* notice, this list of conditions and the following disclaimer.
*
   * Redistributions in binary form must reproduce the above
* copyright notice, this list of conditions and the following disclaimer
* in the documentation and/or other materials provided with the
* distribution.
*   * Neither the name of Google Inc. nor the names of its
* contributors may be used to endorse or promote products derived from
* this software without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
* "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
* LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
* A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT
* OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT

* LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
* DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
* THEORY OF LIABILITY,
 WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
* (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
* OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
*
* curve25519-donna: Curve25519 elliptic curve, public key function
*
* http://code.google.com/p/curve25519-donna/
*
* Adam Langley <agl@imperialviolet.org>
*
* Derived from public domain C code by Daniel J. Bernstein <djb@cr.yp.to>
*
* More information about curve25519 can be found here
*   http://cr.yp.to/ecdh.html
*
* djb's sample implementation of curve25519 is written in a special assembly
* language called qhasm and uses the floating point registers.
*
* This is, almost, a clean room reimplementation from the curve25519 paper. It
* uses many of the tricks described therein. Only the crecip function is taken
* from the sample implementation.
*/

1.22 inetutils 1.9.4

1.22.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for
software and other kinds of works.

The licenses for most software and other practical works are designed
to take away your freedom to share and change the works. By contrast,
the GNU General Public License is intended to guarantee your freedom to
share and change all versions of a program--to make sure it remains free
software for all its users. We, the Free Software Foundation, use the
GNU General Public License for most of our software; it applies also to

any other work released this way by its authors. You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price. Our General Public Licenses
are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
them if you wish), that you receive source code or can get it if you
want it, that you can change the software or use pieces of it in new
free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you
these rights or asking you to surrender the rights. Therefore, you have
certain responsibilities if you distribute copies of the software, or if
you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether
gratis or for a fee, you must pass on to the recipients the same
freedoms that you received. You must make sure that they, too, receive
or can get the source code. And you must show them these terms so they
know their rights.

Developers that use the GNU GPL protect your rights with two steps:
(1) assert copyright on the software, and (2) offer
you this License
giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains
that there is no warranty for this free software. For both users' and
authors' sake, the GPL requires that modified versions be marked as
changed, so that their problems will not be attributed erroneously to
authors of previous versions.

Some devices are designed to deny users access to install or run
modified versions of the software inside them, although the manufacturer
can do so. This is fundamentally incompatible with the aim of
protecting users' freedom to change the software. The systematic
pattern of such abuse occurs in the area of products for individuals to
use, which is precisely where it is most unacceptable. Therefore, we
have designed this version of the GPL to prohibit the practice for those
products. If such problems arise substantially in other domains, we
stand ready to extend this provision to those domains
in future versions
of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents.
States should not allow patents to restrict development and use of
software on general-purpose computers, but in those that do, we wish to

avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify"
a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate
Legal Notices"
to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a

menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than
the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing
those activities but
which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes
a covered work. This License acknowledges your
rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal
Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep

intact all notices stating that this License and any
non-permissive terms added in accord with section 7 apply to the code;
keep intact all notices of the absence of any warranty; and give all
recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey,
and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to
produce it from the Program, in the form of source code under the
terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified
it, and giving a relevant date.

b) The work must carry prominent notices stating that it is
released under this License and any conditions added under section
7. This requirement modifies the requirement in section 4 to
"keep intact all notices".

c) You must license
the entire work, as a whole, under this
License to anyone who comes into possession of a copy. This
License will therefore apply, along with any applicable section 7
additional terms, to the whole of the work, and all its parts,
regardless of how they are packaged. This License gives no
permission to license the work in any other way, but it does not
invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display
Appropriate Legal Notices; however, if the Program has interactive
interfaces that do not display Appropriate Legal Notices, your
work need not make them do so.

A compilation of a covered work with other separate and independent
works, which are not by their nature extensions of the covered work,
and which are not combined with it such as to form a larger program,
in or on a volume of a storage or distribution medium, is called an
"aggregate" if the compilation and its
resulting copyright are not
used to limit the access or legal rights of the compilation's users
beyond what the individual works permit. Inclusion of a covered work
in an aggregate does not cause this License to apply to the other
parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object
code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute
modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does
not include a
requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in
this License, to the extent
that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections
15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that

material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your

receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time
you convey a covered work, the recipient automatically
receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not
impose a license fee, royalty, or other charge for exercise of
rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes
the right to grant
patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other
readily accessible means,
then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended

to all recipients of the covered
work and works based on it.

A patent license is "discriminatory" if it does not include within
the scope of its coverage, prohibits the exercise of, or is
conditioned on the non-exercise of one or more of the rights that are
specifically granted under this License. You may not convey a covered
work if you are a party to an arrangement with a third party that is
in the business of distributing software, under which you make payment
to the third party based on the extent of your activity of conveying
the work, and under which the third party grants, to any of the
parties who would receive the covered work from you, a discriminatory
patent license (a) in connection with copies of the covered work
conveyed by you (or copies made from those copies), or (b) primarily
for and in connection with specific products or compilations that
contain the covered work, unless you entered into that arrangement,
or that patent license was granted, prior to 28 March
2007.

Nothing in this License shall be construed as excluding or limiting
any implied license or other defenses to infringement that may
otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or
otherwise) that contradict the conditions of this License, they do not
excuse you from the conditions of this License. If you cannot convey a
covered work so as to satisfy simultaneously your obligations under this
License and any other pertinent obligations, then as a consequence you may
not convey it at all. For example, if you agree to terms that obligate you
to collect a royalty for further conveying from those to whom you convey
the Program, the only way you could satisfy both those terms and this
License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License,
you have
permission to link or combine any covered work with a work licensed
under version 3 of the GNU Affero General Public License into a single
combined work, and to convey the resulting work. The terms of this
License will continue to apply to the part which is the covered work,
but the special requirements of the GNU Affero General Public License,
section 13, concerning interaction through a network will apply to the
combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF

SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of
warranty and limitation of liability provided
above cannot be given local legal effect according to their terms,
reviewing courts shall apply local law that most closely approximates
an absolute waiver of all civil liability in connection with the
Program, unless a warranty or assumption of liability accompanies a
copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest
possible use to the public, the best way to achieve this is to make it
free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest
to attach them to the start of each source file to most effectively
state the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea
of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation, either version 3 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>

This program comes with ABSOLUTELY
NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what you want to do, use the GNU Lesser General
Public License instead of this License. But first, please
read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.
@c The GNU Free Documentation License.
@center Version 1.3, 3 November 2008

@c This file is intended to be included within another document,
@c hence no sectioning command or @node.

@display
Copyright @copyright{} 2000, 2001, 2002, 2007, 2008 Free Software Foundation, Inc.
@uref{http://fsf.org/}

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.
@end display

@enumerate 0
@item
PREAMBLE

The purpose of this License is to make a manual, textbook, or other
functional and useful document @dfn{free} in the sense of freedom: to
assure everyone the effective freedom to copy and redistribute it,
with or without modifying it, either commercially or noncommercially.
Secondarily, this License preserves for the author and publisher a way
to get credit for their work, while not being considered responsible
for modifications made by others.

This License is a kind of ``copyleft'', which means that derivative

works of the document
must themselves be free in the same sense. It
complements the GNU General Public License, which is a copyleft
license designed for free software.

We have designed this License in order to use it for manuals for free
software, because free software needs free documentation: a free
program should come with manuals providing the same freedoms that the
software does. But this License is not limited to software manuals;
it can be used for any textual work, regardless of subject matter or
whether it is published as a printed book. We recommend this License
principally for works whose purpose is instruction or reference.

@item
APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that
contains a notice placed by the copyright holder saying it can be
distributed under the terms of this License. Such a notice grants a
world-wide, royalty-free license, unlimited in duration, to use that
work under the conditions stated herein. The ``Document'', below,
refers
to any such manual or work. Any member of the public is a
licensee, and is addressed as ``you''. You accept the license if you
copy, modify or distribute the work in a way requiring permission
under copyright law.

A ``Modified Version'' of the Document means any work containing the
Document or a portion of it, either copied verbatim, or with
modifications and/or translated into another language.

A ``Secondary Section'' is a named appendix or a front-matter section
of the Document that deals exclusively with the relationship of the
publishers or authors of the Document to the Document's overall
subject (or to related matters) and contains nothing that could fall
directly within that overall subject. (Thus, if the Document is in
part a textbook of mathematics, a Secondary Section may not explain
any mathematics.) The relationship could be a matter of historical
connection with the subject or with related matters, or of legal,
commercial, philosophical, ethical or political
position regarding
them.

The ``Invariant Sections'' are certain Secondary Sections whose titles
are designated, as being those of Invariant Sections, in the notice
that says that the Document is released under this License. If a
section does not fit the above definition of Secondary then it is not
allowed to be designated as Invariant. The Document may contain zero

Invariant Sections. If the Document does not identify any Invariant
Sections then there are none.

The ``Cover Texts'' are certain short passages of text that are listed,
as Front-Cover Texts or Back-Cover Texts, in the notice that says that
the Document is released under this License. A Front-Cover Text may
be at most 5 words, and a Back-Cover Text may be at most 25 words.

A ``Transparent'' copy of the Document means a machine-readable copy,
represented in a format whose specification is available to the
general public, that is suitable for revising the document
straightforwardly with generic text editors or (for
 images composed of
pixels) generic paint programs or (for drawings) some widely available
drawing editor, and that is suitable for input to text formatters or
for automatic translation to a variety of formats suitable for input
to text formatters. A copy made in an otherwise Transparent file
format whose markup, or absence of markup, has been arranged to thwart
or discourage subsequent modification by readers is not Transparent.
An image format is not Transparent if used for any substantial amount
of text. A copy that is not ``Transparent'' is called ``Opaque''.

Examples of suitable formats for Transparent copies include plain
ASCII without markup, Texinfo input format, La@TeX{} input
format, SGML or XML using a publicly available
DTD, and standard-conforming simple HTML,
PostScript or PDF designed for human modification. Examples
of transparent image formats include PNG, XCF and
JPG@. Opaque formats include proprietary formats that can be
read and edited only by proprietary word
 processors, SGML or
XML for which the DTD and/or processing tools are
not generally available, and the machine-generated HTML,
PostScript or PDF produced by some word processors for
output purposes only.

The ``Title Page'' means, for a printed book, the title page itself,
plus such following pages as are needed to hold, legibly, the material
this License requires to appear in the title page. For works in
formats which do not have any title page as such, ``Title Page'' means
the text near the most prominent appearance of the work's title,
preceding the beginning of the body of the text.

The ``publisher'' means any person or entity that distributes copies
of the Document to the public.

A section ``Entitled XYZ'' means a named subunit of the Document whose
title either is precisely XYZ or contains XYZ in parentheses following

text that translates XYZ in another language. (Here XYZ stands for a
specific section name mentioned below, such as ``Acknowledgements'',
``Dedications'', ``Endorsements'',
 or ``History''.)  To ``Preserve the Title''
of such a section when you modify the Document means that it remains a
section ``Entitled XYZ'' according to this definition.

The Document may include Warranty Disclaimers next to the notice which
states that this License applies to the Document. These Warranty
Disclaimers are considered to be included by reference in this
License, but only as regards disclaiming warranties: any other
implication that these Warranty Disclaimers may have is void and has
no effect on the meaning of this License.

@item
VERBATIM COPYING

You may copy and distribute the Document in any medium, either
commercially or noncommercially, provided that this License, the
copyright notices, and the license notice saying this License applies
to the Document are reproduced in all copies, and that you add no other
conditions whatsoever to those of this License. You may not use
technical measures to obstruct or control the reading or further
copying of the copies
 you make or distribute. However, you may accept
compensation in exchange for copies. If you distribute a large enough
number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and
you may publicly display copies.

@item
COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have
printed covers) of the Document, numbering more than 100, and the
Document's license notice requires Cover Texts, you must enclose the
copies in covers that carry, clearly and legibly, all these Cover
Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on
the back cover. Both covers must also clearly and legibly identify
you as the publisher of these copies. The front cover must present
the full title with all words of the title equally prominent and
visible. You may add other material on the covers in addition.
Copying with changes limited to the covers, as long as they preserve
the
 title of the Document and satisfy these conditions, can be treated
as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit
legibly, you should put the first ones listed (as many as fit
reasonably) on the actual cover, and continue the rest onto adjacent
pages.

If you publish or distribute Opaque copies of the Document numbering
more than 100, you must either include a machine-readable Transparent
copy along with each Opaque copy, or state in or with each Opaque copy
a computer-network location from which the general network-using
public has access to download using public-standard network protocols
a complete Transparent copy of the Document, free of added material.
If you use the latter option, you must take reasonably prudent steps,
when you begin distribution of Opaque copies in quantity, to ensure
that this Transparent copy will remain thus accessible at the stated
location until at least one year after the last time you distribute
 an
Opaque copy (directly or through your agents or retailers) of that
edition to the public.

It is requested, but not required, that you contact the authors of the
Document well before redistributing any large number of copies, to give
them a chance to provide you with an updated version of the Document.

@item
MODIFICATIONS

You may copy and distribute a Modified Version of the Document under
the conditions of sections 2 and 3 above, provided that you release
the Modified Version under precisely this License, with the Modified
Version filling the role of the Document, thus licensing distribution
and modification of the Modified Version to whoever possesses a copy
of it. In addition, you must do these things in the Modified Version:

@enumerate A
@item
Use in the Title Page (and on the covers, if any) a title distinct
from that of the Document, and from those of previous versions
(which should, if there were any, be listed in the History section
of the Document). You may use the same
 title as a previous version
if the original publisher of that version gives permission.

@item
List on the Title Page, as authors, one or more persons or entities
responsible for authorship of the modifications in the Modified
Version, together with at least five of the principal authors of the
Document (all of its principal authors, if it has fewer than five),
unless they release you from this requirement.

@item
State on the Title page the name of the publisher of the
Modified Version, as the publisher.

@item
Preserve all the copyright notices of the Document.

@item
Add an appropriate copyright notice for your modifications
adjacent to the other copyright notices.

@item
Include, immediately after the copyright notices, a license notice
giving the public permission to use the Modified Version under the
terms of this License, in the form shown in the Addendum below.

@item
Preserve in that license notice the full lists of Invariant Sections
and required Cover Texts given in the
Document's license notice.

@item
Include an unaltered copy of this License.

@item
Preserve the section Entitled ``History'', Preserve its Title, and add
to it an item stating at least the title, year, new authors, and
publisher of the Modified Version as given on the Title Page. If
there is no section Entitled ``History'' in the Document, create one
stating the title, year, authors, and publisher of the Document as
given on its Title Page, then add an item describing the Modified
Version as stated in the previous sentence.

@item
Preserve the network location, if any, given in the Document for
public access to a Transparent copy of the Document, and likewise
the network locations given in the Document for previous versions
it was based on. These may be placed in the ``History'' section.
You may omit a network location for a work that was published at
least four years before the Document itself, or if the original
publisher of the version it refers to gives permission.

@item
For any
section Entitled ``Acknowledgements'' or ``Dedications'', Preserve
the Title of the section, and preserve in the section all the
substance and tone of each of the contributor acknowledgements and/or

dedications given therein.

@item
Preserve all the Invariant Sections of the Document,
unaltered in their text and in their titles. Section numbers
or the equivalent are not considered part of the section titles.

@item
Delete any section Entitled ``Endorsements". Such a section
may not be included in the Modified Version.

@item
Do not retitle any existing section to be Entitled ``Endorsements" or
to conflict in title with any Invariant Section.

@item
Preserve any Warranty Disclaimers.
@end enumerate

If the Modified Version includes new front-matter sections or
appendices that qualify as Secondary Sections and contain no material
copied from the Document, you may at your option designate some or all
of these sections as invariant. To do this, add their titles to the
list of Invariant
 Sections in the Modified Version's license notice.
These titles must be distinct from any other section titles.

You may add a section Entitled ``Endorsements", provided it contains
nothing but endorsements of your Modified Version by various
parties---for example, statements of peer review or that the text has
been approved by an organization as the authoritative definition of a
standard.

You may add a passage of up to five words as a Front-Cover Text, and a
passage of up to 25 words as a Back-Cover Text, to the end of the list
of Cover Texts in the Modified Version. Only one passage of
Front-Cover Text and one of Back-Cover Text may be added by (or
through arrangements made by) any one entity. If the Document already
includes a cover text for the same cover, previously added by you or
by arrangement made by the same entity you are acting on behalf of,
you may not add another; but you may replace the old one, on explicit
permission from the previous publisher that added the old
 one.

The author(s) and publisher(s) of the Document do not by this License
give permission to use their names for publicity for or to assert or
imply endorsement of any Modified Version.

@item
COMBINING DOCUMENTS

You may combine the Document with other documents released under this
License, under the terms defined in section 4 above for modified
versions, provided that you include in the combination all of the
Invariant Sections of all of the original documents, unmodified, and
list them all as Invariant Sections of your combined work in its
license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and
multiple identical Invariant Sections may be replaced with a single
copy. If there are multiple Invariant Sections with the same name but
different contents, make the title of each such section unique by
adding at the end of it, in parentheses, the name of the original
author or publisher of that section if
 known, or else a unique number.
Make the same adjustment to the section titles in the list of
Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled ``History''
in the various original documents, forming one section Entitled
``History''; likewise combine any sections Entitled ``Acknowledgements'',
and any sections Entitled ``Dedications''. You must delete all
sections Entitled ``Endorsements.''

@item
COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents
released under this License, and replace the individual copies of this
License in the various documents with a single copy that is included in
the collection, provided that you follow the rules of this License for
verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute
it individually under this License, provided you insert a copy of this
License
 into the extracted document, and follow this License in all
other respects regarding verbatim copying of that document.

@item
AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate
and independent documents or works, in or on a volume of a storage or
distribution medium, is called an ``aggregate'' if the copyright
resulting from the compilation is not used to limit the legal rights

of the compilation's users beyond what the individual works permit.
When the Document is included in an aggregate, this License does not
apply to the other works in the aggregate which are not themselves
derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these
copies of the Document, then if the Document is less than one half of
the entire aggregate, the Document's Cover Texts may be placed on
covers that bracket the Document within the aggregate, or the
electronic equivalent of covers if the Document is in electronic
form.
Otherwise they must appear on printed covers that bracket the whole
aggregate.

@item
TRANSLATION

Translation is considered a kind of modification, so you may
distribute translations of the Document under the terms of section 4.
Replacing Invariant Sections with translations requires special
permission from their copyright holders, but you may include
translations of some or all Invariant Sections in addition to the
original versions of these Invariant Sections. You may include a
translation of this License, and all the license notices in the
Document, and any Warranty Disclaimers, provided that you also include
the original English version of this License and the original versions
of those notices and disclaimers. In case of a disagreement between
the translation and the original version of this License or a notice
or disclaimer, the original version will prevail.

If a section in the Document is Entitled ``Acknowledgements",
``Dedications", or ``History", the requirement
(section 4) to Preserve
its Title (section 1) will typically require changing the actual
title.

@item
TERMINATION

You may not copy, modify, sublicense, or distribute the Document
except as expressly provided under this License. Any attempt
otherwise to copy, modify, sublicense, or distribute it is void, and
will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license
from a particular copyright holder is reinstated (a) provisionally,
unless and until the copyright holder explicitly and finally
terminates your license, and (b) permanently, if the copyright holder

fails to notify you of the violation by some reasonable means prior to
60 days after the cessation.

Moreover, your license from a particular copyright holder is
reinstated permanently if the copyright holder notifies you of the
violation by some reasonable means, this is the first time you have
received notice of violation of this License (for
 any work) from that
copyright holder, and you cure the violation prior to 30 days after
your receipt of the notice.

Termination of your rights under this section does not terminate the
licenses of parties who have received copies or rights from you under
this License. If your rights have been terminated and not permanently
reinstated, receipt of a copy of some or all of the same material does
not give you any rights to use it.

@item
FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions
of the GNU Free Documentation License from time to time. Such new
versions will be similar in spirit to the present version, but may
differ in detail to address new problems or concerns. See
@uref{http://www.gnu.org/copyleft/}.

Each version of the License is given a distinguishing version number.
If the Document specifies that a particular numbered version of this
License ``or any later version'' applies to it, you have the option of
following the terms and
 conditions either of that specified version or
of any later version that has been published (not as a draft) by the
Free Software Foundation. If the Document does not specify a version
number of this License, you may choose any version ever published (not
as a draft) by the Free Software Foundation. If the Document
specifies that a proxy can decide which future versions of this
License can be used, that proxy's public statement of acceptance of a
version permanently authorizes you to choose that version for the
Document.

@item
RELICENSING

``Massive Multiauthor Collaboration Site'' (or ``MMC Site'') means any
World Wide Web server that publishes copyrightable works and also
provides prominent facilities for anybody to edit those works. A
public wiki that anybody can edit is an example of such a server. A
``Massive Multiauthor Collaboration'' (or ``MMC'') contained in the

site means any set of copyrightable works thus published on the MMC site.

``CC-BY-SA'' means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

``Incorporate'' means to publish or republish a Document, in whole or in part, as part of another Document.

An MMC is ``eligible for relicensing'' if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.

@end enumerate

@page
@heading ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

@smallexample
@group
 Copyright (C) @var{year} @var{your name}.
 Permission is granted to copy, distribute and/or modify this document
 under the terms of the GNU Free Documentation License, Version 1.3
 or any later version published by the Free Software Foundation;
 with no Invariant Sections, no Front-Cover Texts, and no Back-Cover
 Texts. A copy of the license is included in the section entitled ``GNU
 Free Documentation License''.
@end group
@end smallexample

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the ``with@dots{}Texts.''@: line with this:

@smallexample
@group
  with the Invariant Sections being @var{list their titles}, with
  the Front-Cover Texts being @var{list}, and with the Back-Cover Texts
  being @var{list}.
@end group
@end smallexample

If you have Invariant
 Sections without Cover Texts, or some other
combination of the three, merge those two alternatives to suit the
situation.

If your document contains nontrivial examples of program code, we
recommend releasing these examples in parallel under your choice of
free software license, such as the GNU General Public License,
to permit their use in free software.

@c Local Variables:
@c ispell-local-pdict: "ispell-dict"
@c End:

1.23 ntp 4.2.8p10

1.23.1 Available under license :

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<meta http-equiv="content-type" content="text/html;charset=iso-8859-1">
<title>Copyright Notice</title>
<!-- Changed by: Harlan Stenn, 10-Mar-2014 -->
<link href="scripts/style.css" type="text/css" rel="stylesheet">
</head>
<body>
<h3>Copyright Notice</h3>
<img src="pic/sheepb.jpg" alt="jpg" align="left"> "Clone me," says Dolly sheepishly.
Last update:
 <!-- #BeginDate format:En2m -->2-Jan-2017 11:58<!-- #EndDate -->
  UTC
<br clear="left">

<hr>
The following copyright notice applies to all files collectively called the Network Time Protocol Version 4 Distribution. Unless specifically declared otherwise in an individual file, this entire notice applies as if the text was explicitly included in the file.
<pre>
****

```
*                                                                      *
* Copyright (c)
 University of Delaware 1992-2015                    *
*                                                                      *
* Permission to use, copy, modify, and distribute this software and   *
* its documentation for any purpose with or without fee is hereby     *
* granted, provided that the above copyright notice appears in all    *
* copies and that both the copyright notice and this permission       *
* notice appear in supporting documentation, and that the name        *
* University of Delaware not be used in advertising or publicity      *
* pertaining to distribution of the software without specific,        *
* written prior permission. The University of Delaware makes no       *
* representations about the suitability this software for any         *
* purpose. It is provided "as is" without express or implied          *
* warranty.                                                           *
*
   *
************************************************************************
</pre>
<p>Content starting in 2011 from Harlan Stenn, Danny Mayer, and Martin Burnicki is:</p>
<pre>
************************************************************************
*                                                                      *
* Copyright (c) Network Time Foundation 2011-2017                     *
*                                                                      *
* All Rights Reserved                                                  *
*                                                                      *
* Redistribution and use in source and binary forms, with or without  *
* modification, are permitted provided that the following conditions  *
* are met:                                                            *
* 1. Redistributions of source code must retain the above copyright   *
*    notice, this list of conditions and the following disclaimer.    *
* 2. Redistributions
 in binary form must reproduce the above                *
*    copyright notice, this list of conditions and the following      *
*    disclaimer in the documentation and/or other materials provided  *
*    with the distribution.                                           *
*                                                                      *
* THIS SOFTWARE IS PROVIDED BY THE AUTHORS ``AS IS" AND ANY EXPRESS   *
* OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED   *
* WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE  *
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE    *
* LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR *
* CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT   *
* OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR  *
* BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF          *
* LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
```

*
* (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE *
* USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH *
* DAMAGE. *
****
</pre>
The following individuals contributed in part to the Network Time Protocol Distribution Version 4 and are acknowledged as authors of this work.

Takao Abe <takao_abe@xurb.jp> Clock driver for JJY receivers
Mark Andrews <mark_andrews@isc.org> Leitch atomic clock controller
Bernd Altmeier <altmeier@atlsoft.de> hopf Elektronik serial line and PCI-bus devices
Viraj Bais <vbais@mailman1.intel.com> and Clayton Kirkwood
<kirkwood@striderfm.intel.com> port to WindowsNT 3.5
Michael Barone <michael,barone@lmco.com> GPSVME fixes
Karl Berry <karl@owl.HQ.ileaf.com> syslog to file option
Greg Brackley <greg.brackley@bigfoot.com> Major rework of WINNT port. Clean up recvbuf and iosignal code into separate modules.
Marc Brett <Marc.Brett@westgeo.com> Magnavox GPS clock driver
Piete Brooks <Piete.Brooks@cl.cam.ac.uk> MSF clock driver, Trimble PARSE support
Nelson B Bolyard <nelson@bolyard.me> update and complete broadcast and crypto features in sntp
Jean-Francois Boudreault <Jean-Francois.Boudreault@viagenie.qc.ca>
IPv6 support
Reg Clemens <reg@dwf.com> Oncore driver (Current maintainer)
Steve Clift <clift@ml.csiro.au> OMEGA clock driver
Casey Crellin <casey@csc.co.za> vxWorks (Tornado) port and help with target configuration
Sven Dietrich <sven_dietrich@trimble.com> Palisade reference clock driver, NT adj. residuals, integrated Greg's Winnt port.
John A. Dundas III <dundas@salt.jpl.nasa.gov> Apple A/UX port
Torsten Duwe <duwe@immd4.informatik.uni-erlangen.de> Linux port
Dennis Ferguson <dennis@mrbill.canet.ca> foundation code for NTP Version 2 as specified
in RFC-1119
John Hay <jhay@icomtek.csir.co.za> IPv6 support and

testing
Dave Hart <davehart@davehart.com> General maintenance, Windows port interpolation rewrite
Claas Hilbrecht <neoclock4x@linum.com> NeoClock4X clock driver
Glenn Hollinger <glenn@herald.usask.ca> GOES clock driver
Mike Iglesias <iglesias@uci.edu> DEC Alpha port
Jim Jagielski <jim@jagubox.gsfc.nasa.gov> A/UX port
Jeff Johnson <jbj@chatham.usdesign.com> massive prototyping overhaul
Hans Lambermont <Hans.Lambermont@nl.origin-it.com> or <H.Lambermont@chello.nl>
ntpsweep
Poul-Henning Kamp <phk@FreeBSD.ORG> Oncore driver (Original author)
Frank Kardel <kardel (at) ntp (dot) org> PARSE <GENERIC> (driver 14 reference clocks), STREAMS modules for PARSE, support scripts, syslog cleanup, dynamic interface handling
Johannes Maximilian Kuehn <kuehn@ntp.org> Rewrote <tt>sntp</tt> to comply with NTPv4 specification, <tt>ntpq saveconfig</tt>
William L. Jones <jones@hermes.chpc.utexas.edu> RS/6000 AIX modifications, HPUX modifications
Dave Katz <dkatz@cisco.com> RS/6000 AIX port
Craig Leres <leres@ee.lbl.gov>
4.4BSD port, ppsclock, Magnavox GPS clock driver
George Lindholm <lindholm@ucs.ubc.ca> SunOS 5.1 port
Louis A. Mamakos <louie@ni.umd.edu> MD5-based authentication
Lars H. Mathiesen <thorinn@diku.dk> adaptation of foundation code for Version 3 as specified in RFC-1305
Danny Mayer <mayer@ntp.org>Network I/O, Windows Port, Code Maintenance
David L. Mills <mills@udel.edu> Version 4 foundation, precision kernel; clock drivers: 1, 3, 4, 6, 7, 11, 13, 18, 19, 22, 36
Wolfgang Moeller <moeller@gwdgv1.dnet.gwdg.de> VMS port
Jeffrey Mogul <mogul@pa.dec.com> ntptrace utility
Tom
Moore <tmoore@fievel.daytonoh.ncr.com> i386 svr4 port
Kamal A Mostafa <kamal@whence.com> SCO OpenServer port
Derek Mulcahy <derek@toybox.demon.co.uk> and Damon Hart-Davis <d@hd.org> ARCRON MSF clock driver
Rob Neal <neal@ntp.org> Bancomm refclock and config/parse code maintenance

Rainer Pruy <Rainer.Pruy@informatik.uni-erlangen.de> monitoring/trap scripts, statistics file handling
Dirce Richards <dirce@zk3.dec.com> Digital UNIX V4.0 port
Wilfredo Sánchez <wsanchez@apple.com> added support for NetInfo
Nick Sayer <mrapple@quack.kfu.com>
SunOS streams modules
Jack Sasportas <jack@innovativeinternet.com> Saved a Lot of space on the stuff in the html/pic/ subdirectory
Ray Schnitzler <schnitz@unipress.com> Unixware1 port
Michael Shields <shields@tembel.org> USNO clock driver
Jeff Steinman <jss@pebbles.jpl.nasa.gov> Datum PTS clock driver
Harlan Stenn <harlan@pfcs.com> GNU automake/autoconfigure makeover, various other bits (see the ChangeLog)
Kenneth Stone <ken@sdd.hp.com> HP-UX port
Ajit Thyagarajan <ajit@ee.udel.edu>IP multicast/anycast support
Tomoaki TSURUOKA <tsuruoka@nc.fukuoka-u.ac.jp>TRAK
clock driver
Brian Utterback <brian.utterback@oracle.com> General codebase, Solaris issues
Loganaden Velvindron <loganaden@gmail.com> Sandboxing (libseccomp) support
Paul A Vixie <vixie@vix.com> TrueTime GPS driver, generic TrueTime clock driver
Ulrich Windl <Ulrich.Windl@rz.uni-regensburg.de> corrected and validated HTML documents according to the HTML DTD

<hr>
</body>
</html>
This file is automatically generated from html/copyright.html

Copyright Notice

jpg "Clone me," says Dolly sheepishly.

Last update: 2-Jan-2017 11:58 UTC

The following copyright notice applies to all files collectively
called the Network Time Protocol Version 4 Distribution. Unless
specifically declared otherwise in an individual file, this entire

notice applies as if the text was explicitly included in the file.

```
**********************************************************************
*                                                                    *
* Copyright (c) University of Delaware 1992-2015                     *
*                                                                    *
* Permission to use, copy, modify, and distribute this software and  *
* its documentation for any purpose with or without fee is hereby    *
* granted, provided that the above
 copyright notice appears in all   *
* copies and that both the copyright notice and this permission      *
* notice appear in supporting documentation, and that the name       *
* University of Delaware not be used in advertising or publicity     *
* pertaining to distribution of the software without specific,       *
* written prior permission. The University of Delaware makes no      *
* representations about the suitability this software for any        *
* purpose. It is provided "as is" without express or implied         *
* warranty.                                                          *
*                                                                    *
**********************************************************************
```

Content starting in 2011 from Harlan Stenn, Danny Mayer, and Martin Burnicki is:

```
**********************************************************************
*
    *
* Copyright (c) Network Time Foundation 2011-2017                    *
*                                                                    *
* All Rights Reserved                                                *
*                                                                    *
* Redistribution and use in source and binary forms, with or without *
* modification, are permitted provided that the following conditions *
* are met:                                                           *
* 1. Redistributions of source code must retain the above copyright  *
*    notice, this list of conditions and the following disclaimer.   *
* 2. Redistributions in binary form must reproduce the above         *
*    copyright notice, this list of conditions and the following     *
*    disclaimer in the documentation and/or other materials provided *
*    with the distribution.                                          *
*
                    *
* THIS SOFTWARE IS PROVIDED BY THE AUTHORS ``AS IS'' AND ANY EXPRESS  *
* OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED  *
* WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE *
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE   *
* LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR *
* CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT  *
* OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR *
* BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF         *
```

* LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT *
* (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE *
* USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH *
* DAMAGE. *
****

The following individuals
contributed in part to the Network Time
Protocol Distribution Version 4 and are acknowledged as authors of
this work.

1. [1]Takao Abe <takao_abe@xurb.jp> Clock driver for JJY receivers
2. [2]Mark Andrews <mark_andrews@isc.org> Leitch atomic clock
   controller
3. [3]Bernd Altmeier <altmeier@atlsoft.de> hopf Elektronik serial
   line and PCI-bus devices
4. [4]Viraj Bais <vbais@mailman1.intel.com> and [5]Clayton Kirkwood
   <kirkwood@striderfm.intel.com> port to WindowsNT 3.5
5. [6]Michael Barone <michael,barone@lmco.com> GPSVME fixes
6. [7]Karl Berry <karl@owl.HQ.ileaf.com> syslog to file option
7. [8]Greg Brackley <greg.brackley@bigfoot.com> Major rework of WINNT
   port. Clean up recvbuf and iosignal code into separate modules.
8. [9]Marc Brett <Marc.Brett@westgeo.com> Magnavox GPS clock driver
9. [10]Piete Brooks <Piete.Brooks@cl.cam.ac.uk> MSF clock driver,
   Trimble PARSE support
10. [11]Nelson
B Bolyard <nelson@bolyard.me> update and complete
   broadcast and crypto features in sntp
11. [12]Jean-Francois Boudreault
   <Jean-Francois.Boudreault@viagenie.qc.ca> IPv6 support
12. [13]Reg Clemens <reg@dwf.com> Oncore driver (Current maintainer)
13. [14]Steve Clift <clift@ml.csiro.au> OMEGA clock driver
14. [15]Casey Crellin <casey@csc.co.za> vxWorks (Tornado) port and
   help with target configuration
15. [16]Sven Dietrich <sven_dietrich@trimble.com> Palisade reference
   clock driver, NT adj. residuals, integrated Greg's Winnt port.
16. [17]John A. Dundas III <dundas@salt.jpl.nasa.gov> Apple A/UX port
17. [18]Torsten Duwe <duwe@immd4.informatik.uni-erlangen.de> Linux
   port
18. [19]Dennis Ferguson <dennis@mrbill.canet.ca> foundation code for
   NTP Version 2 as specified in RFC-1119
19. [20]John Hay <jhay@icomtek.csir.co.za> IPv6 support and testing
20. [21]Dave Hart <davehart@davehart.com> General maintenance,
Windows
   port interpolation rewrite
21. [22]Claas Hilbrecht <neoclock4x@linum.com> NeoClock4X clock driver
22. [23]Glenn Hollinger <glenn@herald.usask.ca> GOES clock driver
23. [24]Mike Iglesias <iglesias@uci.edu> DEC Alpha port
24. [25]Jim Jagielski <jim@jagubox.gsfc.nasa.gov> A/UX port

25. [26]Jeff Johnson <jbj@chatham.usdesign.com> massive prototyping overhaul
26. [27]Hans Lambermont <Hans.Lambermont@nl.origin-it.com> or [28]<H.Lambermont@chello.nl> ntpsweep
27. [29]Poul-Henning Kamp <phk@FreeBSD.ORG> Oncore driver (Original author)
28. [30]Frank Kardel [31]<kardel (at) ntp (dot) org> PARSE <GENERIC> (driver 14 reference clocks), STREAMS modules for PARSE, support scripts, syslog cleanup, dynamic interface handling
29. [32]Johannes Maximilian Kuehn <kuehn@ntp.org> Rewrote sntp to comply with NTPv4 specification, ntpq saveconfig
30. [33]William L. Jones <jones@hermes.chpc.utexas.edu> RS/6000 AIX modifications, HPUX modifications
31. [34]Dave Katz <dkatz@cisco.com> RS/6000 AIX port
32. [35]Craig Leres <leres@ee.lbl.gov> 4.4BSD port, ppsclock, Magnavox GPS clock driver
33. [36]George Lindholm <lindholm@ucs.ubc.ca> SunOS 5.1 port
34. [37]Louis A. Mamakos <louie@ni.umd.edu> MD5-based authentication
35. [38]Lars H. Mathiesen <thorinn@diku.dk> adaptation of foundation code for Version 3 as specified in RFC-1305
36. [39]Danny Mayer <mayer@ntp.org>Network I/O, Windows Port, Code Maintenance
37. [40]David L. Mills <mills@udel.edu> Version 4 foundation, precision kernel; clock drivers: 1, 3, 4, 6, 7, 11, 13, 18, 19, 22, 36
38. [41]Wolfgang Moeller <moeller@gwdgv1.dnet.gwdg.de> VMS port
39. [42]Jeffrey Mogul <mogul@pa.dec.com> ntptrace utility
40. [43]Tom Moore <tmoore@fievel.daytonoh.ncr.com> i386 svr4 port
41. [44]Kamal A Mostafa <kamal@whence.com> SCO OpenServer port
42. [45]Derek Mulcahy <derek@toybox.demon.co.uk> and [46]Damon Hart-Davis <d@hd.org> ARCRON MSF clock driver
43. [47]Rob Neal <neal@ntp.org> Bancomm refclock and config/parse code maintenance
44. [48]Rainer Pruy <Rainer.Pruy@informatik.uni-erlangen.de> monitoring/trap scripts, statistics file handling
45. [49]Dirce Richards <dirce@zk3.dec.com> Digital UNIX V4.0 port
46. [50]Wilfredo Snchez <wsanchez@apple.com> added support for NetInfo
47. [51]Nick Sayer <mrapple@quack.kfu.com> SunOS streams modules
48. [52]Jack Sasportas <jack@innovativeinternet.com> Saved a Lot of space on the stuff in the html/pic/ subdirectory
49. [53]Ray Schnitzler <schnitz@unipress.com> Unixware1 port
50. [54]Michael Shields <shields@tembel.org> USNO clock driver
51. [55]Jeff Steinman <jss@pebbles.jpl.nasa.gov> Datum PTS clock driver
52. [56]Harlan Stenn <harlan@pfcs.com> GNU automake/autoconfigure

makeover, various other bits

(see the ChangeLog)

53. [57]Kenneth Stone <ken@sdd.hp.com> HP-UX port
54. [58]Ajit Thyagarajan <ajit@ee.udel.edu>IP multicast/anycast support
55. [59]Tomoaki TSURUOKA <tsuruoka@nc.fukuoka-u.ac.jp>TRAK clock driver
56. [60]Brian Utterback <brian.utterback@oracle.com> General codebase, Solaris issues
57. [61]Loganaden Velvindron <loganaden@gmail.com> Sandboxing (libseccomp) support
58. [62]Paul A Vixie <vixie@vix.com> TrueTime GPS driver, generic TrueTime clock driver
59. [63]Ulrich Windl <Ulrich.Windl@rz.uni-regensburg.de> corrected and validated HTML documents according to the HTML DTD

References

1. mailto:%20takao_abe@xurb.jp
2. mailto:%20mark_andrews@isc.org
3. mailto:%20altmeier@atlsoft.de
4. mailto:%20vbais@mailman1.intel.co
5. mailto:%20kirkwood@striderfm.intel.com
6. mailto:%20michael.barone@lmco.com
7. mailto:%20karl@owl.HQ.ileaf.com
8. mailto:%20greg.brackley@bigfoot.com
9. mailto:%20Marc.Brett@westgeo.com
10. mailto:%20Piete.Brooks@cl.cam.ac.uk
11. mailto:%20nelson@bolyard.me
12. mailto:%20Jean-Francois.Boudreault@viagenie.qc.ca
13. mailto:%20reg@dwf.com
14. mailto:%20clift@ml.csiro.au
15. mailto:%20casey@csc.co.za
16. mailto:%20Sven_Dietrich@trimble.COM
17. mailto:%20dundas@salt.jpl.nasa.gov
18. mailto:%20duwe@immd4.informatik.uni-erlangen.de
19. mailto:%20dennis@mrbill.canet.ca
20. mailto:%20jhay@icomtek.csir.co.za
21. mailto:%20davehart@davehart.com
22. mailto:%20neoclock4x@linum.com
23. mailto:%20glenn@herald.usask.ca
24. mailto:%20iglesias@uci.edu
25. mailto:%20jagubox.gsfc.nasa.gov
26. mailto:%20jbj@chatham.usdesign.com
27. mailto:%20Hans.Lambermont@nl.origin-it.com
28. mailto:H.Lambermont@chello.nl

29. mailto:%20phk@FreeBSD.ORG
30. http://www4.informatik.uni-erlangen.de/%7ekardel
31. mailto:%20kardel%20%28at%29%20ntp%20%28dot%29%20org
32. mailto:kuehn@ntp.org
33. mailto:%20jones@hermes.chpc.utexas.edu
34. mailto:%20dkatz@cisco.com
35. mailto:%20leres@ee.lbl.gov
36. mailto:%20lindholm@ucs.ubc.ca
37. mailto:%20louie@ni.umd.edu
38. mailto:%20thorinn@diku.dk
39. mailto:%20mayer@ntp.org
40. mailto:%20mills@udel.edu
41. mailto:%20moeller@gwdgv1.dnet.gwdg.de
42. mailto:%20mogul@pa.dec.com
43. mailto:%20tmoore@fievel.daytonoh.ncr.com
44. mailto:%20kamal@whence.com
45. mailto:%20derek@toybox.demon.co.uk
46. mailto:%20d@hd.org
47. mailto:%20neal@ntp.org
48. mailto:%20Rainer.Pruy@informatik.uni-erlangen.de
49. mailto:%20dirce@zk3.dec.com
50. mailto:%20wsanchez@apple.com
51. mailto:%20mrapple@quack.kfu.com
52. mailto:%20jack@innovativeinternet.com
53. mailto:%20schnitz@unipress.com
54. mailto:%20shields@tembel.org
55. mailto:%20pebbles.jpl.nasa.gov
56. mailto:%20harlan@pfcs.com
57. mailto:%20ken@sdd.hp.com
58. mailto:%20ajit@ee.udel.edu
59. mailto:%20tsuruoka@nc.fukuoka-u.ac.jp
60. mailto:%20brian.utterback@oracle.com
61. mailto:%20loganaden@gmail.com
62. mailto:%20vixie@vix.com
63. mailto:%20Ulrich.Windl@rz.uni-regensburg.de

Libevent is available for use under the following license, commonly known as the 3-clause (or "modified") BSD license:

==========

Copyright (c) 2000-2007 Niels Provos <provos@citi.umich.edu>
Copyright (c) 2007-2012 Niels Provos and Nick Mathewson

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright

notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products
derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF
THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
==========

Portions of Libevent are based on works by others, also made available by
them under the three-clause BSD license above. The copyright notices are
available in the corresponding source files; the license is as above. Here's
a list:

log.c:
Copyright (c) 2000 Dug Song <dugsong@monkey.org>
Copyright (c) 1993 The Regents
of the University of California.

strlcpy.c:
Copyright (c) 1998 Todd C. Miller <Todd.Miller@courtesan.com>

win32select.c:
Copyright (c) 2003 Michael A. Davis <mike@datanerds.net>

evport.c:
Copyright (c) 2007 Sun Microsystems

ht-internal.h:
Copyright (c) 2002 Christopher Clark

minheap-internal.h:
Copyright (c) 2006 Maxim Yegorushkin <maxim.yegorushkin@gmail.com>

==========

The arc4module is available under the following, sometimes called the
"OpenBSD" license:

Copyright (c) 1996, David Mazieres <dm@uun.org>
Copyright (c) 2008, Damien Miller <djm@openbsd.org>

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES
WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES
OF
MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR
ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF
OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

==========

The Windows timer code is based on code from libutp, which is
distributed under this license, sometimes called the "MIT" license.

Copyright (c) 2010 BitTorrent, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the
following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.
Copyright (c) 2010 Serge A. Zaitsev

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell

copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN
CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.
Copyright (C) 1992-2015 by Bruce Korb - all rights reserved
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above
   copyright notice, this list of conditions and the following
   disclaimer in the documentation and/or other materials provided
   with the distribution.

3. The name of the author may not be used to endorse or promote
   products derived from this software without specific prior
   written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS" AND ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
DISCLAIMED. IN NO EVENT SHALL THE AUTHOR
BE LIABLE FOR ANY DIRECT,
INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES
(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING
IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

1.24 sqlite 3.23.1

1.24.1 Available under license :

The author disclaims copyright to this source code. In place of
a legal notice, here is a blessing:

May you do good and not evil.
May you find forgiveness for yourself and forgive others.
May you share freely, never taking more than you give.

1.25 libtool 2.4.6

1.25.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it. (Some other Free Software Foundation software is covered by
the GNU Lesser General Public License instead.) You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price.
Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid
anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate to certain responsibilities for you if you
distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether
gratis or for a fee, you must give the recipients all the rights that
you have. You must make sure that they, too, receive or can get the

source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate

copyright notice and disclaimer of warranty; keep intact all the
notices that refer to this License and to the absence of any warranty;
and give any other recipients of the Program a copy of this License
along with the Program.

You may charge a fee for the physical act of transferring a copy, and
you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion
of it, thus forming a work based on the Program, and copy and
distribute such modifications or work under the terms of Section 1
above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices
stating that you changed the files and the date of any change.

b) You must cause
any work that you distribute or publish, that in
whole or in part contains or is derived from the Program or any
part thereof, to be licensed as a whole at no charge to all third
parties under the terms of this License.

c) If the modified program normally reads commands interactively
when run, you must cause it, when started running for such
interactive use in the most ordinary way, to print or display an
announcement including an appropriate copyright notice and a
notice that there is no warranty (or else, saying that you provide
a warranty) and that users may redistribute the program under
these conditions, and telling the user how to view a copy of this
License. (Exception: if the Program itself is interactive but
does not normally print such an announcement, your work based on
the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If
identifiable sections of that work
are not derived from the Program,
and can be reasonably considered independent and separate works in
themselves, then this License, and its terms, do not apply to those
sections when you distribute them as separate works. But when you
distribute the same sections as part of a whole which is a work based
on the Program, the distribution of the whole must be on the terms of
this License, whose permissions for other licensees extend to the
entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest
your rights to work written entirely by you; rather, the intent is to
exercise the right to control the distribution of derivative or
collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt

otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made

generous contributions to the wide range of software distributed
through that system in reliance on consistent application of that
system; it is up to the author/donor to
decide if he or she is willing
to distribute software through any other system and a licensee cannot
impose that choice.

This section is intended to make thoroughly clear what is believed to
be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in
certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Program under this License
may add an explicit geographical distribution limitation excluding
those countries, so that distribution is permitted only in or among
countries not thus excluded. In such case, this License incorporates
the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions
of the General Public License from time to time. Such new versions will
be similar in spirit to the present version, but may differ in detail to
address new problems or concerns.

Each version is given a distinguishing
version number. If the Program
specifies a version number of this License which applies to it and "any
later version", you have the option of following the terms and conditions
either of that version or of any later version published by the Free
Software Foundation. If the Program does not specify a version number of
this License, you may choose any version ever published by the Free Software
Foundation.

10. If you wish to incorporate parts of the Program into other free
programs whose distribution conditions are different, write to the author
to ask for permission. For software which is copyrighted by the Free
Software Foundation, write to the Free Software Foundation; we sometimes
make exceptions for this. Our decision will be guided by the two goals
of preserving the free status of all derivatives of our free software and
of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE,
THERE IS NO WARRANTY
FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES
PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED
OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF

MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR
THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU
General Public License as published by
the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

  Gnomovision version 69, Copyright (C) year name of author
  Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
  This is free software, and you are welcome to redistribute
it
  under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

 Yoyodyne, Inc., hereby disclaims all copyright interest in the program
 `Gnomovision' (which makes passes at compilers) written by James Hacker.

 <signature of Ty Coon>, 1 April 1989
 Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this
 is what you want to do, use the GNU Lesser General
Public License instead of this License.
                GNU LESSER GENERAL PUBLIC LICENSE
                   Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts
as the successor of the GNU Library Public License, version 2, hence
the version number 2.1.]

                        Preamble

 The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
Licenses are intended to guarantee your freedom to share and change

free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that

any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits
such linking only if the
entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting
the free library to free
software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact

all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that

uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate
properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally
distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on

the Library and of the other library facilities is otherwise
permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work
based on the Library, uncombined with any
other library
facilities. This must be distributed under the terms of the
Sections above.

b) Give prominent notice with the combined library of the fact
that part of it is a work based on the Library, and explaining
where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute
the Library except as expressly provided under this License. Any
attempt otherwise to copy, modify, sublicense, link with, or
distribute the Library is void, and will automatically terminate your
rights under this License. However, parties who have received copies,
or rights, from you under this License will not have their licenses
terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not
signed it. However, nothing else grants you permission to modify or
distribute the Library or its derivative works. These actions are
prohibited by law if
you do not accept this License. Therefore, by
modifying or distributing the Library (or any work based on the
Library), you indicate your acceptance of this License to do so, and
all its terms and conditions for copying, distributing or modifying
the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the
Library), the recipient automatically receives a license from the
original licensor to copy, distribute, link with or modify the Library
subject to these terms and conditions. You may not impose any further
restrictions on the recipients' exercise of the rights granted herein.
You are not responsible for enforcing compliance by third parties with
this License.

11. If, as a consequence of a court judgment or allegation of patent
infringement or for any other reason (not limited to patent issues),
conditions are imposed on you (whether by court order, agreement or
otherwise) that contradict the conditions of this License, they do not
excuse
you from the conditions of this License. If you cannot
distribute so as to satisfy simultaneously your obligations under this
License and any other pertinent obligations, then as a consequence you
may not distribute the Library at all. For example, if a patent

license would not permit royalty-free redistribution of the Library by
all those who receive copies directly or indirectly through you, then
the only way you could satisfy both it and this License would be to
refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any
particular circumstance, the balance of the section is intended to apply,
and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any
patents or other property right claims or to contest validity of any
such claims; this section has the sole purpose of protecting the
integrity of the free software distribution system
 which is
implemented by public license practices. Many people have made
generous contributions to the wide range of software distributed
through that system in reliance on consistent application of that
system; it is up to the author/donor to decide if he or she is willing
to distribute software through any other system and a licensee cannot
impose that choice.

This section is intended to make thoroughly clear what is believed to
be a consequence of the rest of this License.

 12. If the distribution and/or use of the Library is restricted in
certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Library under this License may add
an explicit geographical distribution limitation excluding those countries,
so that distribution is permitted only in or among countries not thus
excluded. In such case, this License incorporates the limitation as if
written in the body of this License.

 13. The Free Software Foundation may publish
 revised and/or new
versions of the Lesser General Public License from time to time.
Such new versions will be similar in spirit to the present version,
but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library
specifies a version number of this License which applies to it and
"any later version", you have the option of following the terms and
conditions either of that version or of any later version published by
the Free Software Foundation. If the Library does not specify a
license version number, you may choose any version ever published by
the Free Software Foundation.

 14. If you wish to incorporate parts of the Library into other free
programs whose distribution conditions are incompatible with these,

write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision
will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE,
BE LIABLE TO YOU
FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey
the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or
modify it under the terms of the GNU Lesser General Public
License as published by the Free Software Foundation; either
version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public
License along with this library; if not, write to the Free Software
Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301
USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the library, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the
library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!
@c The GNU Free Documentation License.
@center Version 1.3, 3 November 2008

@c This file is intended to be included within another document,
@c hence no sectioning command or @node.

@display
Copyright @copyright{} 2000, 2001, 2002, 2007, 2008 Free Software Foundation, Inc.
@uref{http://fsf.org/}

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.
@end display

@enumerate 0
@item
PREAMBLE

The purpose of this License is to make a manual, textbook, or other
functional and useful document @dfn{free} in the sense of freedom: to
assure everyone the effective freedom to copy and redistribute it,
with or without modifying it, either commercially or noncommercially.
Secondarily, this License preserves for the author and publisher a way
to get credit for their work, while not being considered responsible
for modifications made by others.

This License is a kind of ``copyleft'', which means that derivative
works of the document
 must themselves be free in the same sense. It
complements the GNU General Public License, which is a copyleft
license designed for free software.

We have designed this License in order to use it for manuals for free
software, because free software needs free documentation: a free
program should come with manuals providing the same freedoms that the
software does. But this License is not limited to software manuals;
it can be used for any textual work, regardless of subject matter or
whether it is published as a printed book. We recommend this License
principally for works whose purpose is instruction or reference.

@item
APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that
contains a notice placed by the copyright holder saying it can be
distributed under the terms of this License. Such a notice grants a
world-wide, royalty-free license, unlimited in duration, to use that
work under the conditions stated herein. The ``Document'', below,
refers
 to any such manual or work. Any member of the public is a
licensee, and is addressed as ``you''. You accept the license if you
copy, modify or distribute the work in a way requiring permission
under copyright law.

A ``Modified Version'' of the Document means any work containing the
Document or a portion of it, either copied verbatim, or with
modifications and/or translated into another language.

A ``Secondary Section'' is a named appendix or a front-matter section
of the Document that deals exclusively with the relationship of the
publishers or authors of the Document to the Document's overall
subject (or to related matters) and contains nothing that could fall
directly within that overall subject. (Thus, if the Document is in
part a textbook of mathematics, a Secondary Section may not explain
any mathematics.) The relationship could be a matter of historical

connection with the subject or with related matters, or of legal,
commercial, philosophical, ethical or political
position regarding
them.

The ``Invariant Sections'' are certain Secondary Sections whose titles
are designated, as being those of Invariant Sections, in the notice
that says that the Document is released under this License. If a
section does not fit the above definition of Secondary then it is not
allowed to be designated as Invariant. The Document may contain zero
Invariant Sections. If the Document does not identify any Invariant
Sections then there are none.

The ``Cover Texts'' are certain short passages of text that are listed,
as Front-Cover Texts or Back-Cover Texts, in the notice that says that
the Document is released under this License. A Front-Cover Text may
be at most 5 words, and a Back-Cover Text may be at most 25 words.

A ``Transparent'' copy of the Document means a machine-readable copy,
represented in a format whose specification is available to the
general public, that is suitable for revising the document
straightforwardly with generic text editors or (for
images composed of
pixels) generic paint programs or (for drawings) some widely available
drawing editor, and that is suitable for input to text formatters or
for automatic translation to a variety of formats suitable for input
to text formatters. A copy made in an otherwise Transparent file
format whose markup, or absence of markup, has been arranged to thwart
or discourage subsequent modification by readers is not Transparent.
An image format is not Transparent if used for any substantial amount
of text. A copy that is not ``Transparent'' is called ``Opaque''.

Examples of suitable formats for Transparent copies include plain
ASCII without markup, Texinfo input format, La@TeX{} input
format, SGML or XML using a publicly available
DTD, and standard-conforming simple HTML,
PostScript or PDF designed for human modification. Examples
of transparent image formats include PNG, XCF and
JPG@. Opaque formats include proprietary formats that can be
read and edited only by proprietary word
processors, SGML or
XML for which the DTD and/or processing tools are
not generally available, and the machine-generated HTML,
PostScript or PDF produced by some word processors for
output purposes only.

The ``Title Page'' means, for a printed book, the title page itself,
plus such following pages as are needed to hold, legibly, the material

this License requires to appear in the title page. For works in
formats which do not have any title page as such, ``Title Page'' means
the text near the most prominent appearance of the work's title,
preceding the beginning of the body of the text.

The ``publisher'' means any person or entity that distributes copies
of the Document to the public.

A section ``Entitled XYZ'' means a named subunit of the Document whose
title either is precisely XYZ or contains XYZ in parentheses following
text that translates XYZ in another language. (Here XYZ stands for a
specific section name mentioned below, such as ``Acknowledgements'',
``Dedications'', ``Endorsements'',
 or ``History''.)  To ``Preserve the Title''
of such a section when you modify the Document means that it remains a
section ``Entitled XYZ'' according to this definition.

The Document may include Warranty Disclaimers next to the notice which
states that this License applies to the Document. These Warranty
Disclaimers are considered to be included by reference in this
License, but only as regards disclaiming warranties: any other
implication that these Warranty Disclaimers may have is void and has
no effect on the meaning of this License.

@item
VERBATIM COPYING

You may copy and distribute the Document in any medium, either
commercially or noncommercially, provided that this License, the
copyright notices, and the license notice saying this License applies
to the Document are reproduced in all copies, and that you add no other
conditions whatsoever to those of this License. You may not use
technical measures to obstruct or control the reading or further
copying of the copies
 you make or distribute. However, you may accept
compensation in exchange for copies. If you distribute a large enough
number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and
you may publicly display copies.

@item
COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have
printed covers) of the Document, numbering more than 100, and the
Document's license notice requires Cover Texts, you must enclose the
copies in covers that carry, clearly and legibly, all these Cover

Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the
title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute
an
Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

@item
MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

@enumerate A
@item
Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section

of the Document). You may use the same
title as a previous version
if the original publisher of that version gives permission.

@item
List on the Title Page, as authors, one or more persons or entities
responsible for authorship of the modifications in the Modified
Version, together with at least five of the principal authors of the
Document (all of its principal authors, if it has fewer than five),
unless they release you from this requirement.

@item
State on the Title page the name of the publisher of the
Modified Version, as the publisher.

@item
Preserve all the copyright notices of the Document.

@item
Add an appropriate copyright notice for your modifications
adjacent to the other copyright notices.

@item
Include, immediately after the copyright notices, a license notice
giving the public permission to use the Modified Version under the
terms of this License, in the form shown in the Addendum below.

@item
Preserve in that license notice the full lists of Invariant Sections
and required Cover Texts given in the
Document's license notice.

@item
Include an unaltered copy of this License.

@item
Preserve the section Entitled ``History'', Preserve its Title, and add
to it an item stating at least the title, year, new authors, and
publisher of the Modified Version as given on the Title Page. If
there is no section Entitled ``History'' in the Document, create one
stating the title, year, authors, and publisher of the Document as
given on its Title Page, then add an item describing the Modified
Version as stated in the previous sentence.

@item
Preserve the network location, if any, given in the Document for
public access to a Transparent copy of the Document, and likewise
the network locations given in the Document for previous versions

it was based on. These may be placed in the ``History'' section.
You may omit a network location for a work that was published at
least four years before the Document itself, or if the original
publisher of the version it refers to gives permission.

@item
For any
section Entitled ``Acknowledgements'' or ``Dedications'', Preserve
the Title of the section, and preserve in the section all the
substance and tone of each of the contributor acknowledgements and/or
dedications given therein.

@item
Preserve all the Invariant Sections of the Document,
unaltered in their text and in their titles. Section numbers
or the equivalent are not considered part of the section titles.

@item
Delete any section Entitled ``Endorsements''. Such a section
may not be included in the Modified Version.

@item
Do not retitle any existing section to be Entitled ``Endorsements'' or
to conflict in title with any Invariant Section.

@item
Preserve any Warranty Disclaimers.
@end enumerate

If the Modified Version includes new front-matter sections or
appendices that qualify as Secondary Sections and contain no material
copied from the Document, you may at your option designate some or all
of these sections as invariant. To do this, add their titles to the
list of Invariant
Sections in the Modified Version's license notice.
These titles must be distinct from any other section titles.

You may add a section Entitled ``Endorsements'', provided it contains
nothing but endorsements of your Modified Version by various
parties---for example, statements of peer review or that the text has
been approved by an organization as the authoritative definition of a
standard.

You may add a passage of up to five words as a Front-Cover Text, and a
passage of up to 25 words as a Back-Cover Text, to the end of the list
of Cover Texts in the Modified Version. Only one passage of
Front-Cover Text and one of Back-Cover Text may be added by (or
through arrangements made by) any one entity. If the Document already

includes a cover text for the same cover, previously added by you or
by arrangement made by the same entity you are acting on behalf of,
you may not add another; but you may replace the old one, on explicit
permission from the previous publisher that added the old
one.

The author(s) and publisher(s) of the Document do not by this License
give permission to use their names for publicity for or to assert or
imply endorsement of any Modified Version.

@item
COMBINING DOCUMENTS

You may combine the Document with other documents released under this
License, under the terms defined in section 4 above for modified
versions, provided that you include in the combination all of the
Invariant Sections of all of the original documents, unmodified, and
list them all as Invariant Sections of your combined work in its
license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and
multiple identical Invariant Sections may be replaced with a single
copy. If there are multiple Invariant Sections with the same name but
different contents, make the title of each such section unique by
adding at the end of it, in parentheses, the name of the original
author or publisher of that section if
known, or else a unique number.
Make the same adjustment to the section titles in the list of
Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled ``History''
in the various original documents, forming one section Entitled
``History''; likewise combine any sections Entitled ``Acknowledgements'',
and any sections Entitled ``Dedications''. You must delete all
sections Entitled ``Endorsements.''

@item
COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents
released under this License, and replace the individual copies of this
License in the various documents with a single copy that is included in
the collection, provided that you follow the rules of this License for
verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute
it individually under this License, provided you insert a copy of this
License

into the extracted document, and follow this License in all
other respects regarding verbatim copying of that document.

@item
AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate
and independent documents or works, in or on a volume of a storage or
distribution medium, is called an ``aggregate'' if the copyright
resulting from the compilation is not used to limit the legal rights
of the compilation's users beyond what the individual works permit.
When the Document is included in an aggregate, this License does not
apply to the other works in the aggregate which are not themselves
derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these
copies of the Document, then if the Document is less than one half of
the entire aggregate, the Document's Cover Texts may be placed on
covers that bracket the Document within the aggregate, or the
electronic equivalent of covers if the Document is in electronic
form.
Otherwise they must appear on printed covers that bracket the whole
aggregate.

@item
TRANSLATION

Translation is considered a kind of modification, so you may
distribute translations of the Document under the terms of section 4.
Replacing Invariant Sections with translations requires special
permission from their copyright holders, but you may include
translations of some or all Invariant Sections in addition to the
original versions of these Invariant Sections. You may include a
translation of this License, and all the license notices in the
Document, and any Warranty Disclaimers, provided that you also include
the original English version of this License and the original versions
of those notices and disclaimers. In case of a disagreement between
the translation and the original version of this License or a notice
or disclaimer, the original version will prevail.

If a section in the Document is Entitled ``Acknowledgements'',
``Dedications'', or ``History'', the requirement
(section 4) to Preserve
its Title (section 1) will typically require changing the actual
title.

@item
TERMINATION

You may not copy, modify, sublicense, or distribute the Document
except as expressly provided under this License. Any attempt
otherwise to copy, modify, sublicense, or distribute it is void, and
will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license
from a particular copyright holder is reinstated (a) provisionally,
unless and until the copyright holder explicitly and finally
terminates your license, and (b) permanently, if the copyright holder
fails to notify you of the violation by some reasonable means prior to
60 days after the cessation.

Moreover, your license from a particular copyright holder is
reinstated permanently if the copyright holder notifies you of the
violation by some reasonable means, this is the first time you have
received notice of violation of this License (for
 any work) from that
copyright holder, and you cure the violation prior to 30 days after
your receipt of the notice.

Termination of your rights under this section does not terminate the
licenses of parties who have received copies or rights from you under
this License. If your rights have been terminated and not permanently
reinstated, receipt of a copy of some or all of the same material does
not give you any rights to use it.

@item
FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions
of the GNU Free Documentation License from time to time. Such new
versions will be similar in spirit to the present version, but may
differ in detail to address new problems or concerns. See
@uref{http://www.gnu.org/copyleft/}.

Each version of the License is given a distinguishing version number.
If the Document specifies that a particular numbered version of this
License ``or any later version'' applies to it, you have the option of
following the terms and
 conditions either of that specified version or
of any later version that has been published (not as a draft) by the
Free Software Foundation. If the Document does not specify a version
number of this License, you may choose any version ever published (not
as a draft) by the Free Software Foundation. If the Document
specifies that a proxy can decide which future versions of this
License can be used, that proxy's public statement of acceptance of a
version permanently authorizes you to choose that version for the

Document.

@item
RELICENSING

``Massive Multiauthor Collaboration Site'' (or ``MMC Site'') means any
World Wide Web server that publishes copyrightable works and also
provides prominent facilities for anybody to edit those works. A
public wiki that anybody can edit is an example of such a server. A
``Massive Multiauthor Collaboration'' (or ``MMC'') contained in the
site means any set of copyrightable works thus published on the MMC
site.

``CC-BY-SA'' means the Creative Commons
 Attribution-Share Alike 3.0
license published by Creative Commons Corporation, a not-for-profit
corporation with a principal place of business in San Francisco,
California, as well as future copyleft versions of that license
published by that same organization.

``Incorporate'' means to publish or republish a Document, in whole or
in part, as part of another Document.

An MMC is ``eligible for relicensing'' if it is licensed under this
License, and if all works that were first published under this License
somewhere other than this MMC, and subsequently incorporated in whole
or in part into the MMC, (1) had no cover texts or invariant sections,
and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site
under CC-BY-SA on the same site at any time before August 1, 2009,
provided the MMC is eligible for relicensing.

@end enumerate

@page
@heading ADDENDUM: How to use this License for your documents

To use this License
 in a document you have written, include a copy of
the License in the document and put the following copyright and
license notices just after the title page:

@smallexample
@group
 Copyright (C) @var{year} @var{your name}.
 Permission is granted to copy, distribute and/or modify this document
 under the terms of the GNU Free Documentation License, Version 1.3

or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover
Texts. A copy of the license is included in the section entitled ``GNU
Free Documentation License".
@end group
@end smallexample

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts,
replace the ``with@dots{}Texts."@: line with this:

@smallexample
@group
  with the Invariant Sections being @var{list their titles}, with
  the Front-Cover Texts being @var{list}, and with the Back-Cover Texts
  being @var{list}.
@end group
@end smallexample

If you have Invariant
Sections without Cover Texts, or some other
combination of the three, merge those two alternatives to suit the
situation.

If your document contains nontrivial examples of program code, we
recommend releasing these examples in parallel under your choice of
free software license, such as the GNU General Public License,
to permit their use in free software.

@c Local Variables:
@c ispell-local-pdict: "ispell-dict"
@c End:

1.26 libusb 1.0.20

1.26.1 Available under license :

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts
as the successor of the GNU Library Public License, version 2, hence
the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest
you first think carefully about whether
this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients
all the rights that we gave
you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without
limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's

complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based

on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or

linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License.
Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables
containing that work also fall under Section 6,
whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable

source code for the Library including whatever
changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user
installs one, as long as the modified version is
interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major
components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot

distribute
so as to satisfy simultaneously your obligations under this
License and any other pertinent obligations, then as a consequence you
may not distribute the Library at all. For example, if a patent
license would not permit royalty-free redistribution of the Library by
all those who receive copies directly or indirectly through you, then
the only way you could satisfy both it and this License would be to
refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any
particular circumstance, the balance of the section is intended to apply,
and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any
patents or other property right claims or to contest validity of any
such claims; this section has the sole purpose of protecting the
integrity of the free software distribution system which is
implemented by public license practices. Many people
have made
generous contributions to the wide range of software distributed
through that system in reliance on consistent application of that
system; it is up to the author/donor to decide if he or she is willing
to distribute software through any other system and a licensee cannot
impose that choice.

This section is intended to make thoroughly clear what is believed to
be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in
certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Library under this License may add
an explicit geographical distribution limitation excluding those countries,
so that distribution is permitted only in or among countries not thus
excluded. In such case, this License incorporates the limitation as if
written in the body of this License.

13. The Free Software Foundation may publish revised and/or new
versions of the Lesser General Public
License from time to time.
Such new versions will be similar in spirit to the present version,
but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library
specifies a version number of this License which applies to it and
"any later version", you have the option of following the terms and
conditions either of that version or of any later version published by
the Free Software Foundation. If the Library does not specify a
license version number, you may choose any version ever published by

the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively

convey the exclusion of warranty; and each file should have at least the
"copyright" line
and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or
modify it under the terms of the GNU Lesser General Public
License as published by the Free Software Foundation; either
version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public
License along with this library; if not, write to the Free Software
Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should
also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the library, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the
library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

1.27 libyaml 0.1.7

1.27.1 Available under license :

Copyright (c) 2006 Kirill Simonov

Permission is hereby granted, free of charge, to any person obtaining a copy of
this software and associated documentation files (the "Software"), to deal in
the Software without restriction, including without limitation the rights to
use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies
of the Software, and to permit persons to whom the Software is furnished to do
so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all
copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
SOFTWARE.

1.28 ncurses 6.0

1.28.1 Available under license :

Upstream source http://invisible-island.net/ncurses/ncurses-examples.html

Current ncurses maintainer: Thomas Dickey <dickey@invisible-island.net>

Files: *
Copyright: 1998-2014,2015 Free Software Foundation, Inc.
Licence: X11

Files: aclocal.m4 package
Copyright: 2003-2014,2015 by Thomas E. Dickey
Licence: X11

Permission is hereby granted, free of charge, to any person obtaining a
copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, distribute with modifications, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included
in all copies or substantial portions
of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS
OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.
IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM,
DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR
OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR

THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name(s) of the above copyright holders shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization.

Files: install-sh
Copyright: 1994 X Consortium
Licence: X11

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE X CONSORTIUM BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNEC-TION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of the X Consortium shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization from the X Consortium.

FSF changes to this file are in the public domain.

Calling this script install-sh is preferred over install.sh, to prevent `make' implicit rules from creating a file called install from it when there is no Makefile.

This script is compatible with the BSD install script, but was written from scratch. It can only install one file at a time, a restriction shared with many OS's install programs.

On Debian systems, the complete text of the GNU General Public License can be found in '/usr/share/common-licenses/GPL-2'

-- vile: txtmode file-encoding=utf-8
Upstream source http://invisible-island.net/ncurses/ncurses-examples.html

Current ncurses maintainer: Thomas Dickey <dickey@invisible-island.net>

Files: *
Copyright: 1998-2014,2015 Free Software Foundation, Inc.
Licence: X11

Files: aclocal.m4 package
Copyright: 2010-2014,2015 by Thomas E. Dickey
Licence: X11

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, distribute with modifications, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions
of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name(s) of the above copyright holders shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization.

Files: install-sh
Copyright: 1994 X Consortium
Licence: X11

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated

documentation files (the "Software"), to
deal in the Software without restriction, including without limitation the
rights to use, copy, modify, merge, publish, distribute, sublicense, and/or
sell copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
X CONSORTIUM BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN
AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNEC-
TION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name
of the X Consortium shall not
be used in advertising or otherwise to promote the sale, use or other deal-
ings in this Software without prior written authorization from the X Consor-
tium.

FSF changes to this file are in the public domain.

Calling this script install-sh is preferred over install.sh, to prevent
`make' implicit rules from creating a file called install from it
when there is no Makefile.

This script is compatible with the BSD install script, but was written
from scratch. It can only install one file at a time, a restriction
shared with many OS's install programs.

On Debian systems, the complete text of the GNU General
Public License can be found in '/usr/share/common-licenses/GPL-2'

-- vile: txtmode file-encoding=utf-8
Upstream source http://invisible-island.net/ncurses/ncurses.html
This package is used for testing builds of ncurses.

Current ncurses maintainer: Thomas Dickey <dickey@invisible-island.net>

Files: *
Copyright: 1998-2014,2015 Free Software Foundation, Inc.
Licence: X11

Files: aclocal.m4 package
Copyright: 1996-2014,2015 by Thomas E. Dickey

Licence: X11

Files: doc/html/NCURSES-Programming-HOWTO.html
Copyright: 2001 by Pradeep Padala
Licence: X11

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, distribute with modifications, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name(s) of the above copyright holders shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization.

Files: install-sh
Copyright: 1994 X Consortium
Licence: X11

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR

IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE X CONSORTIUM BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT
OF OR IN CONNEC-
TION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of the X Consortium shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization from the X Consortium.

Files: progs/tset.c ncurses/tinfo/read_termcap.c
Copyright: 1980,1991,1992,1993 The Regents of the University of California.
License: BSD

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in
the
documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

-- vile: txtmode file-encoding=utf-8
Copyright (c) 1998-2014,2015 Free Software Foundation, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the

"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, distribute with modifications, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included
in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS
OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.
IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM,
DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR
OTHERWISE,
ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR
THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name(s) of the above copyright
holders shall not be used in advertising or otherwise to promote the
sale, use or other dealings in this Software without prior written
authorization.

-- vile:txtmode fc=72
-- $Id: COPYING,v 1.3 2015/01/03 20:12:01 tom Exp $

1.29 libidn 1.33

1.29.1 Available under license :

GNU LESSER GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates
the terms and conditions of version 3 of the GNU General Public
License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, "this License" refers to version 3 of the GNU Lesser
General Public License, and the "GNU GPL" refers to version 3 of the GNU
General Public License.

"The Library" refers to a covered work governed by this License,
other than an Application or a Combined Work as defined below.

An "Application" is any work that makes use of an interface provided
by the Library, but which is not otherwise based on the Library.
Defining a subclass of a class defined by
the Library is deemed a mode
of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an
Application with the Library. The particular version of the Library
with which the Combined Work was made is also called the "Linked
Version".

The "Minimal Corresponding Source" for a Combined Work means the
Corresponding Source for the Combined Work, excluding any source code
for portions of the Combined Work that, considered in isolation, are
based on the Application, and not on the Linked Version.

The "Corresponding Application Code" for a Combined Work means the
object code and/or source code for the Application, including any data
and utility programs needed for reproducing the Combined Work from the
Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License
without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a
facility refers to a function or data to be supplied by an Application
that uses the facility (other than as an argument passed when the
facility is invoked), then you may convey a copy of the modified
version:

a) under this License, provided that you make a good faith effort to
ensure that, in the event an Application does not supply the
function or data, the facility still operates, and performs
whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of
this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from

a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer

system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you

received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library,
whether gratis
or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software
patents pose a constant threat to the existence of
any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits
such linking only if the
entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less

of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the

Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be
reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary
GNU General Public
License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for

that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may

distribute the
object code for the work under the terms of Section 6.
Any executables containing that work also fall under Section 6,
whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or
link a "work that uses the Library" with the Library to produce a
work containing portions of the Library, and distribute that work
under terms of your choice, provided that the terms permit
modification of the work for the customer's own use and reverse
engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the
Library is used in it and that the Library and its use are covered by
this License. You must supply a copy of this License. If the work
during execution displays copyright notices, you must include the
copyright notice for the Library among them, as well as a reference
directing the user to the copy of this License. Also, you must do one
of these things:

a) Accompany
the work with the complete corresponding
machine-readable source code for the Library including whatever
changes were used in the work (which must be distributed under
Sections 1 and 2 above); and, if the work is an executable linked
with the Library, with the complete machine-readable "work that
uses the Library", as object code and/or source code, so that the
user can modify the Library and then relink to produce a modified
executable containing the modified Library. (It is understood
that the user who changes the contents of definitions files in the
Library will not necessarily be able to recompile the application
to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the
Library. A suitable mechanism is one that (1) uses at run time a
copy of the library already present on the user's computer system,
rather than copying library functions into the executable, and (2)
will operate
properly with a modified version of the library, if
the user installs one, as long as the modified version is
interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at
least three years, to give the same user the materials
specified in Subsection 6a, above, for a charge no more
than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy

from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally
distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any
other library
facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not

signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to

be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY

AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE,
BE LIABLE TO YOU
FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey
the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if

necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the
library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price.

Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and
(2) offer you this license which
gives you legal permission to copy,
distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain
that everyone understands that there is no warranty for this free
software. If the software is modified by someone else and passed on, we
want its recipients to know that what they have is not the original, so
that any problems introduced by others will not reflect on the original
authors' reputations.

Finally, any free program is threatened constantly by software
patents. We wish to avoid the danger that redistributors of a free
program will individually obtain patent licenses, in effect making the
program proprietary. To prevent this, we have made it clear that any
patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and
modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains
a notice placed by the copyright holder saying it may be distributed
under the terms of this General Public License. The "Program", below,
refers to any such program or work, and a "work based on the Program"
means either the Program or any derivative work under copyright law:
that is to say, a work containing the Program or a portion of it,
either verbatim or with modifications and/or translated into another
language. (Hereinafter, translation is included without limitation in
the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not
covered by this License; they are outside its scope. The act of
running the Program is not restricted, and the output from the Program
is covered only if its contents constitute a work based on the
Program (independent of having been made by running the Program).
Whether that is true depends on what the
Program does.

1. You may copy and distribute verbatim copies of the Program's
source code as you receive it, in any medium, provided that you
conspicuously and appropriately publish on each copy an appropriate
copyright notice and disclaimer of warranty; keep intact all the
notices that refer to this License and to the absence of any warranty;
and give any other recipients of the Program a copy of this License

along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of

a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under

this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to

decide if he or she is willing
to distribute software through any other system and a licensee cannot
impose that choice.

This section is intended to make thoroughly clear what is believed to
be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in
certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Program under this License
may add an explicit geographical distribution limitation excluding
those countries, so that distribution is permitted only in or among
countries not thus excluded. In such case, this License incorporates
the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions
of the General Public License from time to time. Such new versions will
be similar in spirit to the present version, but may differ in detail to
address new problems or concerns.

Each version is given a distinguishing
version number. If the Program
specifies a version number of this License which applies to it and "any
later version", you have the option of following the terms and conditions
either of that version or of any later version published by the Free
Software Foundation. If the Program does not specify a version number of
this License, you may choose any version ever published by the Free Software
Foundation.

10. If you wish to incorporate parts of the Program into other free
programs whose distribution conditions are different, write to the author
to ask for permission. For software which is copyrighted by the Free
Software Foundation, write to the Free Software Foundation; we sometimes
make exceptions for this. Our decision will be guided by the two goals
of preserving the free status of all derivatives of our free software and
of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE,
THERE IS NO WARRANTY
FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES
PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED
OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS
TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE
PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING,

REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR
THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU
General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute
it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this
is what you want to do, use the GNU Lesser General
Public License instead of this License.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price.

Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which
gives you legal permission to copy,
distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law:

that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work
are not derived from the Program,
and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution
and only if you
received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to

control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source
code, even though third parties are not
compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing
or modifying
the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For

example, if a patent
license would not permit royalty-free redistribution of the Program by
all those who receive copies directly or indirectly through you, then
the only way you could satisfy both it and this License would be to
refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under
any particular circumstance, the balance of the section is intended to
apply and the section as a whole is intended to apply in other
circumstances.

It is not the purpose of this section to induce you to infringe any
patents or other property right claims or to contest validity of any
such claims; this section has the sole purpose of protecting the
integrity of the free software distribution system, which is
implemented by public license practices. Many people have made
generous contributions to the wide range of software distributed
through that system in reliance on consistent application of that
system; it is up to the author/donor to
decide if he or she is willing
to distribute software through any other system and a licensee cannot
impose that choice.

This section is intended to make thoroughly clear what is believed to
be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in
certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Program under this License
may add an explicit geographical distribution limitation excluding
those countries, so that distribution is permitted only in or among
countries not thus excluded. In such case, this License incorporates
the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions
of the General Public License from time to time. Such new versions will
be similar in spirit to the present version, but may differ in detail to
address new problems or concerns.

Each version is given a distinguishing
version number. If the Program
specifies a version number of this License which applies to it and "any
later version", you have the option of following the terms and conditions
either of that version or of any later version published by the Free
Software Foundation. If the Program does not specify a version number of
this License, you may choose any version ever published by the Free Software
Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU
General Public License as published by
the Free Software Foundation; either version 2 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License along
with this program; if not, write to the Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute
it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this
is what you want to do, use the GNU Lesser General
Public License instead of this License.

License below is copied from <http://www.unicode.org/copyright.html>,
last updated 7 July 2004, and claims to apply to all Unicode versions.

According to a post on emacs-devel,
<http://lists.gnu.org/archive/html/emacs-devel/2004-04/msg00036.html>,
RMS believe it is a free license:

> This is a free license, and even compatible with the GPL (if
> that ever matters). Yes, we can use it now.

EXHIBIT 1
UNICODE, INC. LICENSE AGREEMENT - DATA FILES AND SOFTWARE

Unicode Data Files include all data files under the directories
http://www.unicode.org/Public/ and
http://www.unicode.org/reports/. Unicode Software includes any source
code under the directories http://www.unicode.org/Public/ and
http://www.unicode.org/reports/.

NOTICE TO USER: Carefully read the following legal agreement. BY
DOWNLOADING, INSTALLING, COPYING OR OTHERWISE USING UNICODE INC.'S
DATA FILES ("DATA FILES"), AND/OR SOFTWARE ("SOFTWARE"), YOU
UNEQUIVOCALLY ACCEPT, AND AGREE TO BE BOUND BY, ALL OF THE TERMS AND
CONDITIONS
OF THIS AGREEMENT. IF YOU DO NOT AGREE, DO NOT DOWNLOAD,
INSTALL, COPY, DISTRIBUTE OR USE THE DATA FILES OR SOFTWARE.

COPYRIGHT AND PERMISSION NOTICE

Copyright 1991-2004 Unicode, Inc. All rights reserved. Distributed
under the Terms of Use in http://www.unicode.org/copyright.html.

Permission is hereby granted, free of charge, to any person obtaining
a copy of the Unicode data files and associated documentation (the
"Data Files") or Unicode software and associated documentation (the
"Software") to deal in the Data Files or Software without restriction,
including without limitation the rights to use, copy, modify, merge,
publish, distribute, and/or sell copies of the Data Files or Software,
and to permit persons to whom the Data Files or Software are furnished
to do so, provided that (a) the above copyright notice(s) and this
permission notice appear in all copies of the Data Files or Software,
(b) both the above copyright notice(s) and this permission notice
appear in associated
documentation, and (c) there is clear notice in
each modified Data File or in the Software as well as in the
documentation associated with the Data File(s) or Software that the
data or software has been modified.

THE DATA FILES AND SOFTWARE ARE PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THE DATA FILES OR SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in these Data Files or Software without prior written authorization of the copyright holder.

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical

transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial
revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this
License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made,

use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and
may provide additional or different license terms and conditions

for use, reproduction, or distribution of Your modifications, or
for any such Derivative Works as a whole, provided Your use,
reproduction, and distribution of the Work otherwise complies with
the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise,
any Contribution intentionally submitted for inclusion in the Work
by You to the Licensor shall be under the terms and conditions of
this License, without any additional terms or conditions.
Notwithstanding the above, nothing herein shall supersede or modify
the terms of any separate license agreement you may have executed
with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade
names, trademarks, service marks, or product names of the Licensor,
except as required for reasonable and customary use in describing the
origin of the Work and reproducing the
content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or
agreed to in writing, Licensor provides the Work (and each
Contributor provides its Contributions) on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
implied, including, without limitation, any warranties or conditions
of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A
PARTICULAR PURPOSE. You are solely responsible for determining the
appropriateness of using or redistributing the Work and assume any
risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory,
whether in tort (including negligence), contract, or otherwise,
unless required by applicable law (such as deliberate and grossly
negligent acts) or agreed to in writing, shall any Contributor be
liable to You for damages, including any direct,
indirect, special,
incidental, or consequential damages of any character arising as a
result of this License or out of the use or inability to use the
Work (including but not limited to damages for loss of goodwill,
work stoppage, computer failure or malfunction, or any and all
other commercial damages or losses), even if such Contributor
has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing
the Work or Derivative Works thereof, You may choose to offer,
and charge a fee for, acceptance of support, warranty, indemnity,

or other liability obligations and/or rights consistent with this
License. However, in accepting such obligations, You may act only
on Your own behalf and on Your sole responsibility, not on behalf
of any other Contributor, and only if You agree to indemnify,
defend, and hold each Contributor harmless for any liability
incurred by, or claims asserted against, such Contributor by reason
of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following
boilerplate notice, with the fields enclosed by brackets "[]"
replaced with your own identifying information. (Don't include
the brackets!) The text should be enclosed in the appropriate
comment syntax for the file format. We also recommend that a
file or class name and description of purpose be included on the
same "printed page" as the copyright notice for easier
identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for
software and other kinds of works.

The licenses for most software and other practical works are designed
to take away your freedom to share and change the works. By contrast,

the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to
freedom, not
price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps:
(1)
assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand
ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2)

tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that

same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered
by this License only if the output, given its
content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed;
section 10
makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you

receive it, in any medium, provided that you conspicuously and
appropriately
publish on each copy an appropriate copyright notice;
keep intact all notices stating that this License and any
non-permissive terms added in accord with section 7 apply to the code;
keep intact all notices of the absence of any warranty; and give all
recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey,
and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to
produce it from the Program, in the form of source code under the
terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified
it, and giving a relevant date.

b) The work must carry prominent notices stating that it is
released under this License and any conditions added under section
7. This requirement modifies the requirement in section
4 to
"keep intact all notices".

c) You must license the entire work, as a whole, under this
License to anyone who comes into possession of a copy. This
License will therefore apply, along with any applicable section 7
additional terms, to the whole of the work, and all its parts,
regardless of how they are packaged. This License gives no
permission to license the work in any other way, but it does not
invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display
Appropriate Legal Notices; however, if the Program has interactive
interfaces that do not display Appropriate Legal Notices, your
work need not make them do so.

A compilation of a covered work with other separate and independent
works, which are not by their nature extensions of the covered work,
and which are not combined with it such as to form a larger program,
in or on a volume of a storage or distribution
medium, is called an
"aggregate" if the compilation and its resulting copyright are not
used to limit the access or legal rights of the compilation's users
beyond what the individual works permit. Inclusion of a covered work
in an aggregate does not cause this License to apply to the other

parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided

you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and

adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some

trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on

those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above
requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that

copyright
holder, and you cure the violation prior to 30 days after
your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights
granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify

or convey a specific copy of the covered
work, then the patent license
you grant is automatically extended to all recipients of the covered
work and works based on it.

A patent license is "discriminatory" if it does not include within
the scope of its coverage, prohibits the exercise of, or is
conditioned on the non-exercise of one or more of the rights that are
specifically granted under this License. You may not convey a covered
work if you are a party to an arrangement with a third party that is
in the business of distributing software, under which you make payment
to the third party based on the extent of your activity of conveying
the work, and under which the third party grants, to any of the
parties who would receive the covered work from you, a discriminatory
patent license (a) in connection with copies of the covered work
conveyed by you (or copies made from those copies), or (b) primarily
for and in connection with specific products or compilations that
contain the covered work, unless you entered into that arrangement,
or
that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting
any implied license or other defenses to infringement that may
otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or
otherwise) that contradict the conditions of this License, they do not
excuse you from the conditions of this License. If you cannot convey a
covered work so as to satisfy simultaneously your obligations under this
License and any other pertinent obligations, then as a consequence you may
not convey it at all. For example, if you agree to terms that obligate you
to collect a royalty for further conveying from those to whom you convey
the Program, the only way you could satisfy both those terms and this
License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have
permission to link or combine any covered work with a work licensed
under version 3 of the GNU Affero General Public License into a single
combined work, and to convey the resulting work. The terms of this
License will continue to apply to the part which is the covered work,
but the special requirements of the GNU Affero General Public License,
section 13, concerning interaction through a network will apply to the
combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS),

EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17.
Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>
This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what you want to
do, use the GNU Lesser General
Public License instead of this License. But first, please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.
@c The GNU Free Documentation License.
@center Version 1.3, 3 November 2008

@c This file is intended to be included within another document,
@c hence no sectioning command or @node.

@display
Copyright @copyright{} 2000, 2001, 2002, 2007, 2008 Free Software Foundation, Inc.
@uref{http://fsf.org/}

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.
@end display

@enumerate 0
@item
PREAMBLE

The purpose of this License is to make a manual, textbook, or other
functional and useful document @dfn{free} in the sense of freedom: to
assure everyone the effective freedom to copy and redistribute it,
with or without modifying it, either commercially or noncommercially.
Secondarily, this License preserves for the author and publisher a way
to get credit for their work, while not being considered responsible
for modifications made by others.

This License is a kind of ``copyleft'', which means that derivative works of the document
must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

@item
APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The ``Document'', below, refers
to any such manual or work. Any member of the public is a licensee, and is addressed as ``you''. You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A ``Modified Version'' of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A ``Secondary Section'' is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political
position regarding
them.

The ``Invariant Sections'' are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not

allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The ``Cover Texts'' are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A ``Transparent'' copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not ``Transparent'' is called ``Opaque''.

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, La@TeX{} input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG@. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The ``Title Page'' means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, ``Title Page'' means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

The ``publisher'' means any person or entity that distributes copies of the Document to the public.

A section ``Entitled XYZ'' means a named subunit of the Document whose

title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as ``Acknowledgements'', ``Dedications'', ``Endorsements'', or ``History''.) To ``Preserve the Title'' of such a section when you modify the Document means that it remains a section ``Entitled XYZ'' according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

@item
VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

@item
COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit
legibly, you should put the first ones listed (as many as fit
reasonably) on the actual cover, and continue the rest onto adjacent
pages.

If you publish or distribute Opaque copies of the Document numbering
more than 100, you must either include a machine-readable Transparent
copy along with each Opaque copy, or state in or with each Opaque copy
a computer-network location from which the general network-using
public has access to download using public-standard network protocols
a complete Transparent copy of the Document, free of added material.
If you use the latter option, you must take reasonably prudent steps,
when you begin distribution of Opaque copies in quantity, to ensure
that this Transparent copy will remain thus accessible at the stated
location until at least one year after the last time you distribute
 an
Opaque copy (directly or through your agents or retailers) of that
edition to the public.

It is requested, but not required, that you contact the authors of the
Document well before redistributing any large number of copies, to give
them a chance to provide you with an updated version of the Document.

@item
MODIFICATIONS

You may copy and distribute a Modified Version of the Document under
the conditions of sections 2 and 3 above, provided that you release
the Modified Version under precisely this License, with the Modified
Version filling the role of the Document, thus licensing distribution
and modification of the Modified Version to whoever possesses a copy
of it. In addition, you must do these things in the Modified Version:

@enumerate A
@item
Use in the Title Page (and on the covers, if any) a title distinct
from that of the Document, and from those of previous versions
(which should, if there were any, be listed in the History section
of the Document). You may use the same
 title as a previous version
if the original publisher of that version gives permission.

@item
List on the Title Page, as authors, one or more persons or entities
responsible for authorship of the modifications in the Modified
Version, together with at least five of the principal authors of the
Document (all of its principal authors, if it has fewer than five),

unless they release you from this requirement.

@item
State on the Title page the name of the publisher of the
Modified Version, as the publisher.

@item
Preserve all the copyright notices of the Document.

@item
Add an appropriate copyright notice for your modifications
adjacent to the other copyright notices.

@item
Include, immediately after the copyright notices, a license notice
giving the public permission to use the Modified Version under the
terms of this License, in the form shown in the Addendum below.

@item
Preserve in that license notice the full lists of Invariant Sections
and required Cover Texts given in the
Document's license notice.

@item
Include an unaltered copy of this License.

@item
Preserve the section Entitled ``History'', Preserve its Title, and add
to it an item stating at least the title, year, new authors, and
publisher of the Modified Version as given on the Title Page. If
there is no section Entitled ``History'' in the Document, create one
stating the title, year, authors, and publisher of the Document as
given on its Title Page, then add an item describing the Modified
Version as stated in the previous sentence.

@item
Preserve the network location, if any, given in the Document for
public access to a Transparent copy of the Document, and likewise
the network locations given in the Document for previous versions
it was based on. These may be placed in the ``History'' section.
You may omit a network location for a work that was published at
least four years before the Document itself, or if the original
publisher of the version it refers to gives permission.

@item
For any
section Entitled ``Acknowledgements'' or ``Dedications'', Preserve
the Title of the section, and preserve in the section all the

substance and tone of each of the contributor acknowledgements and/or
dedications given therein.

@item
Preserve all the Invariant Sections of the Document,
unaltered in their text and in their titles. Section numbers
or the equivalent are not considered part of the section titles.

@item
Delete any section Entitled ``Endorsements". Such a section
may not be included in the Modified Version.

@item
Do not retitle any existing section to be Entitled ``Endorsements" or
to conflict in title with any Invariant Section.

@item
Preserve any Warranty Disclaimers.
@end enumerate

If the Modified Version includes new front-matter sections or
appendices that qualify as Secondary Sections and contain no material
copied from the Document, you may at your option designate some or all
of these sections as invariant. To do this, add their titles to the
list of Invariant
 Sections in the Modified Version's license notice.
These titles must be distinct from any other section titles.

You may add a section Entitled ``Endorsements", provided it contains
nothing but endorsements of your Modified Version by various
parties---for example, statements of peer review or that the text has
been approved by an organization as the authoritative definition of a
standard.

You may add a passage of up to five words as a Front-Cover Text, and a
passage of up to 25 words as a Back-Cover Text, to the end of the list
of Cover Texts in the Modified Version. Only one passage of
Front-Cover Text and one of Back-Cover Text may be added by (or
through arrangements made by) any one entity. If the Document already
includes a cover text for the same cover, previously added by you or
by arrangement made by the same entity you are acting on behalf of,
you may not add another; but you may replace the old one, on explicit
permission from the previous publisher that added the old
 one.

The author(s) and publisher(s) of the Document do not by this License
give permission to use their names for publicity for or to assert or
imply endorsement of any Modified Version.

@item
COMBINING DOCUMENTS

You may combine the Document with other documents released under this
License, under the terms defined in section 4 above for modified
versions, provided that you include in the combination all of the
Invariant Sections of all of the original documents, unmodified, and
list them all as Invariant Sections of your combined work in its
license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and
multiple identical Invariant Sections may be replaced with a single
copy. If there are multiple Invariant Sections with the same name but
different contents, make the title of each such section unique by
adding at the end of it, in parentheses, the name of the original
author or publisher of that section if
 known, or else a unique number.
Make the same adjustment to the section titles in the list of
Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled ``History"
in the various original documents, forming one section Entitled
``History"; likewise combine any sections Entitled ``Acknowledgements",
and any sections Entitled ``Dedications". You must delete all
sections Entitled ``Endorsements."

@item
COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents
released under this License, and replace the individual copies of this
License in the various documents with a single copy that is included in
the collection, provided that you follow the rules of this License for
verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute
it individually under this License, provided you insert a copy of this
License
 into the extracted document, and follow this License in all
other respects regarding verbatim copying of that document.

@item
AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate
and independent documents or works, in or on a volume of a storage or
distribution medium, is called an ``aggregate" if the copyright

resulting from the compilation is not used to limit the legal rights
of the compilation's users beyond what the individual works permit.
When the Document is included in an aggregate, this License does not
apply to the other works in the aggregate which are not themselves
derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these
copies of the Document, then if the Document is less than one half of
the entire aggregate, the Document's Cover Texts may be placed on
covers that bracket the Document within the aggregate, or the
electronic equivalent of covers if the Document is in electronic
 form.
Otherwise they must appear on printed covers that bracket the whole
aggregate.

@item
TRANSLATION

Translation is considered a kind of modification, so you may
distribute translations of the Document under the terms of section 4.
Replacing Invariant Sections with translations requires special
permission from their copyright holders, but you may include
translations of some or all Invariant Sections in addition to the
original versions of these Invariant Sections. You may include a
translation of this License, and all the license notices in the
Document, and any Warranty Disclaimers, provided that you also include
the original English version of this License and the original versions
of those notices and disclaimers. In case of a disagreement between
the translation and the original version of this License or a notice
or disclaimer, the original version will prevail.

If a section in the Document is Entitled ``Acknowledgements'',
``Dedications'', or ``History'', the requirement
 (section 4) to Preserve
its Title (section 1) will typically require changing the actual
title.

@item
TERMINATION

You may not copy, modify, sublicense, or distribute the Document
except as expressly provided under this License. Any attempt
otherwise to copy, modify, sublicense, or distribute it is void, and
will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license
from a particular copyright holder is reinstated (a) provisionally,
unless and until the copyright holder explicitly and finally

terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for
 any work) from that
copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

@item
FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See @uref{http://www.gnu.org/copyleft/}.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License ``or any later version'' applies to it, you have the option of following the terms and
 conditions either of that specified version or
of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

@item
RELICENSING

``Massive Multiauthor Collaboration Site'' (or ``MMC Site'') means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A

``Massive Multiauthor Collaboration" (or ``MMC") contained in the
site means any set of copyrightable works thus published on the MMC
site.

``CC-BY-SA" means the Creative Commons
 Attribution-Share Alike 3.0
license published by Creative Commons Corporation, a not-for-profit
corporation with a principal place of business in San Francisco,
California, as well as future copyleft versions of that license
published by that same organization.

``Incorporate" means to publish or republish a Document, in whole or
in part, as part of another Document.

An MMC is ``eligible for relicensing" if it is licensed under this
License, and if all works that were first published under this License
somewhere other than this MMC, and subsequently incorporated in whole
or in part into the MMC, (1) had no cover texts or invariant sections,
and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site
under CC-BY-SA on the same site at any time before August 1, 2009,
provided the MMC is eligible for relicensing.

@end enumerate

@page
@heading ADDENDUM: How to use this License for your documents

To use this License
 in a document you have written, include a copy of
the License in the document and put the following copyright and
license notices just after the title page:

@smallexample
@group
 Copyright (C) @var{year} @var{your name}.
 Permission is granted to copy, distribute and/or modify this document
 under the terms of the GNU Free Documentation License, Version 1.3
 or any later version published by the Free Software Foundation;
 with no Invariant Sections, no Front-Cover Texts, and no Back-Cover
 Texts. A copy of the license is included in the section entitled ``GNU
 Free Documentation License".
@end group
@end smallexample

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts,
replace the ``with@dots{}Texts."@: line with this:

@smallexample
@group
  with the Invariant Sections being @var{list their titles}, with
  the Front-Cover Texts being @var{list}, and with the Back-Cover Texts
  being @var{list}.
@end group
@end smallexample

If you have Invariant
 Sections without Cover Texts, or some other
combination of the three, merge those two alternatives to suit the
situation.

If your document contains nontrivial examples of program code, we
recommend releasing these examples in parallel under your choice of
free software license, such as the GNU General Public License,
to permit their use in free software.

@c Local Variables:
@c ispell-local-pdict: "ispell-dict"
@c End:
Libidn COPYING -- Explanation of licensing conditions.
Copyright (C) 2002-2015 Simon Josefsson
See the end for copying conditions.

The source code for the C library (libidn.a or libidn.so), the C#
library (Libidn.dll) and the Java library (libidn-*.jar) are licensed
under the terms of either the GNU General Public License version 2.0
or later (see the file COPYINGv2) or the GNU Lesser General Public
License version 3.0 or later (see the file COPYING.LESSERv3), or both
in parallel as here.

The author of the Java library has agreed to also distribute it under
the Apache License Version 2.0 (see the file java/LICENSE-2.0).

The manual is licensed under the GNU Free Documentation License,
Version 1.3 or any later.

The command line tool, self tests, examples, and other auxilliary
files, are licensed under the GNU General Public License version 3.0
or later.

Other files are licensed as indicated in each file.

There may be exceptions to these general rules, see each file for
precise information.

Copying
and distribution of this file, with or without modification,
are permitted in any medium without royalty provided the copyright
notice and this notice are preserved.

1.30 zlib 1.2.3

1.30.1 Available under license :

/* zlib.h -- interface of the 'zlib' general purpose compression library
version 1.2.11, January 15th, 2017

Copyright (C) 1995-2017 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied
warranty. In no event will the authors be held liable for any damages
arising from the use of this software.

Permission is granted to anyone to use this software for any purpose,
including commercial applications, and to alter it and redistribute it
freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not
claim that you wrote the original software. If you use this software
in a product, an acknowledgment in the product documentation would be
appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be
misrepresented as being the original software.
3. This notice may not be removed or altered from any source
distribution.

Jean-loup Gailly Mark Adler
jloup@gzip.org madler@alumni.caltech.edu

*/
Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization
obtaining a copy of the software and accompanying documentation covered by
this license (the "Software") to use, reproduce, display, distribute,
execute, and transmit the Software, and to prepare derivative works of the
Software, and to permit third-parties to whom the Software is furnished to
do so, all subject to the following:

The copyright notices in the Software and this entire statement, including
the above license grant, this restriction and the following disclaimer,
must be included in all copies of the Software, in whole or in part, and

all derivative works of the Software, unless such copies or derivative
works are solely in the form of machine-executable object code generated by
a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES
OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

1.31 zlib 1.2.8

1.31.1 Available under license :

/* zlib.h -- interface of the 'zlib' general purpose compression library
version 1.2.11, January 15th, 2017

Copyright (C) 1995-2017 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied
warranty. In no event will the authors be held liable for any damages
arising from the use of this software.

Permission is granted to anyone to use this software for any purpose,
including commercial applications, and to alter it and redistribute it
freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not
claim that you wrote the original software. If you use this software
in a product, an acknowledgment in the product documentation would be
appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be
misrepresented as being the original software.
3. This notice may not be removed or altered from any source
distribution.

Jean-loup Gailly Mark Adler
jloup@gzip.org madler@alumni.caltech.edu

*/
Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization
obtaining a copy of the software and accompanying documentation covered by
this license (the "Software") to use, reproduce, display, distribute,

execute, and transmit the Software, and to prepare derivative works of the
Software, and to permit third-parties to whom the Software is furnished to
do so, all subject to the following:

The copyright notices in the Software and this entire statement, including
the above license grant, this restriction and the following disclaimer,
must be included in all copies of the Software, in whole or in part, and
all derivative works of the Software, unless such copies or derivative
works are solely in the form of machine-executable object code generated by
a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES
OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT
SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE
FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE,
ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER
DEALINGS IN THE SOFTWARE.

1.32 gawk 4.1.3

1.32.1 Available under license :

GNU LIBRARY GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the library GPL. It is
numbered 2 because it goes with version 2 of the ordinary GPL.]

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
Licenses are intended to guarantee your freedom to share and change
free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some
specially designated Free Software Foundation software, and to any
other libraries whose authors decide to use it. You can use it for
your libraries, too.

When we speak of free software, we are referring to freedom,

not
price. Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid
anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate to certain responsibilities for you if
you distribute copies of the library, or if you modify it.

For example, if you distribute copies of the library, whether gratis
or for a fee, you must give the recipients all the rights that we gave
you. You must make sure that they, too, receive or can get the source
code. If you link a program with the library, you must provide
complete object files to the recipients so that they can relink them
with the library, after making
changes to the library and recompiling
it. And you must show them these terms so they know their rights.

Our method of protecting your rights has two steps: (1) copyright
the library, and (2) offer you this license which gives you legal
permission to copy, distribute and/or modify the library.

Also, for each distributor's protection, we want to make certain
that everyone understands that there is no warranty for this free
library. If the library is modified by someone else and passed on, we
want its recipients to know that what they have is not the original
version, so that any problems introduced by others will not reflect on
the original authors' reputations.

Finally, any free program is threatened constantly by software
patents. We wish to avoid the danger that companies distributing free
software will individually obtain patent licenses, thus in effect
transforming the program into proprietary software. To prevent this,
we have made it clear that any patent must be licensed
for everyone's
free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary
GNU General Public License, which was designed for utility programs. This
license, the GNU Library General Public License, applies to certain
designated libraries. This license is quite different from the ordinary
one; be sure to read it in full, and don't assume that anything in it is
the same as in the ordinary license.

The reason we have a separate public license for some libraries is that

they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and legal sense, the linked executable is a combined work, a derivative of the original library, and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public License for libraries did not effectively promote software sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

GNU LIBRARY GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work

which has been distributed
under these terms. A "work based on the
Library" means either the Library or any derivative work under
copyright law: that is to say, a work containing the Library or a
portion of it, either verbatim or with modifications and/or translated
straightforwardly into another language. (Hereinafter, translation is
included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for
making modifications to it. For a library, complete source code means
all the source code for all modules it contains, plus any associated
interface definition files, plus the scripts used to control compilation
and installation of the library.

Activities other than copying, distribution and modification are not
covered by this License; they are outside its scope. The act of
running a program using the Library is not restricted, and output from
such a program is covered only if its contents constitute a work based
on the Library (independent
of the use of the Library in a tool for
writing it). Whether that is true depends on what the Library does
and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's
complete source code as you receive it, in any medium, provided that
you conspicuously and appropriately publish on each copy an
appropriate copyright notice and disclaimer of warranty; keep intact
all the notices that refer to this License and to the absence of any
warranty; and distribute a copy of this License along with the
Library.

You may charge a fee for the physical act of transferring a copy,
and you may at your option offer warranty protection in exchange for a
fee.

2. You may modify your copy or copies of the Library or any portion
of it, thus forming a work based on the Library, and copy and
distribute such modifications or work under the terms of Section 1
above, provided that you also meet all of these conditions:

a) The modified work must
itself be a software library.

b) You must cause the files modified to carry prominent notices
stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no
charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also compile or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply
a copy of this License. If the work
during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Accompany the
work with a written offer, valid for at
least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

c) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

d) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the

Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute
the Library at all. For example, if a patent
license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system;
it is up to the author/donor to decide if he or she is willing
to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if

written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Library General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH

DAMAGES.

END OF TERMS AND CONDITIONS

Appendix: How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year>
<name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Library General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Library General Public License for more details.

You should have received a copy of the GNU Library General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary.
Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for
software and other kinds of works.

The licenses for most software and other practical works are designed
to take away your freedom to share and change the works. By contrast,
the GNU General Public License is intended to guarantee your freedom to
share and change all versions of a program--to make sure it remains free
software for all its users. We, the Free Software Foundation, use the
GNU General Public License for most of our software; it applies also to
any other work released this way by its authors. You can apply it to
your programs, too.

When we speak of free software, we are referring to
freedom, not
price. Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
them if you wish), that you receive source code or can get it if you
want it, that you can change the software or use pieces of it in new
free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you
these rights or asking you to surrender the rights. Therefore, you have
certain responsibilities if you distribute copies of the software, or if
you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether
gratis or for a fee, you must pass on to the recipients the same
freedoms that you received. You must make sure that they, too, receive
or can get the source code. And you must show them these terms so they
know their rights.

Developers that use the GNU GPL protect your rights with two steps:
(1)
assert copyright on the software, and (2) offer you this License
giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains

that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand
ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees"
and
"recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to

control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological

measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately
publish on each copy an appropriate copyright notice;
keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to
"keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not

invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated
place (gratis or for a charge), and offer equivalent access to the
Corresponding Source in
the same way through the same place at no
further charge. You need not require recipients to copy the
Corresponding Source along with the object code. If the place to
copy the object code is a network server, the Corresponding Source
may be on a different server (operated by you or a third party)
that supports equivalent copying facilities, provided you maintain
clear directions next to the object code saying where to find the
Corresponding Source. Regardless of what server hosts the
Corresponding Source, you remain obligated to ensure that it is
available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided
you inform other peers where the object code and Corresponding
Source of the work are being offered to the general public at no
charge under subsection 6d.

A separable portion of the object code, whose source code is excluded
from the Corresponding Source
as a System Library, need not be
included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any
tangible personal property which is normally used for personal, family,
or household purposes, or (2) anything designed or sold for incorporation
into a dwelling. In determining whether a product is a consumer product,
doubtful cases shall be resolved in favor of coverage. For a particular
product received by a particular user, "normally used" refers to a
typical or common use of that class of product, regardless of the status
of the particular user or of the way in which the particular user
actually uses, or expects or is expected to use, the product. A product
is a consumer product regardless of whether the product has substantial
commercial, industrial or non-consumer uses, unless such uses represent
the only significant mode of use of the product.

"Installation Information" for a User Product means any methods,
procedures, authorization
keys, or other information required to install
and execute modified versions of a covered work in that User Product from
a modified version of its Corresponding Source. The information must
suffice to ensure that the continued functioning of the modified object
code is in no case prevented or interfered with solely because
modification has been made.

If you convey an object code work under this section in, or with, or

specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in
ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the
entire Program shall
be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or
limiting liability differently from the
terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or
author attributions in that material or in the Appropriate Legal
Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or
requiring that modified versions of such material be marked in
reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or
authors of the material; or

e) Declining to grant rights under trademark law for use of some
trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that
material by anyone who conveys the material (or modified versions of
it) with contractual assumptions of liability to the recipient, for
any liability that these contractual assumptions directly impose on

those licensors and authors.

All other non-permissive additional terms are considered "further
restrictions" within the meaning of section 10. If the Program as you
received it, or any part of it, contains a notice stating that it is
governed by this License along with a term that is a further
restriction, you may remove that term. If a license document contains
a further restriction but permits relicensing or conveying under this
License, you may add to a covered work material governed by the terms
of that license document, provided that the further restriction does
not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you
must place, in the relevant source files, a statement of the
additional terms that apply to those files, or a notice indicating
where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the
form of a separately written license, or stated as exceptions;
the above
requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly

provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright
holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered

work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights
granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For
purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this

License, through a
publicly available network server or other readily accessible means,
then you must either (1) cause the Corresponding Source to be so
available, or (2) arrange to deprive yourself of the benefit of the
patent license for this particular work, or (3) arrange, in a manner
consistent with the requirements of this License, to extend the patent
license to downstream recipients. "Knowingly relying" means you have
actual knowledge that, but for the patent license, your conveying the
covered work in a country, or your recipient's use of the covered work
in a country, would infringe one or more identifiable patents in that
country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or
arrangement, you convey, or propagate by procuring conveyance of, a
covered work, and grant a patent license to some of the parties
receiving the covered work authorizing them to use, propagate, modify
or convey a specific copy of the covered
work, then the patent license
you grant is automatically extended to all recipients of the covered
work and works based on it.

A patent license is "discriminatory" if it does not include within
the scope of its coverage, prohibits the exercise of, or is
conditioned on the non-exercise of one or more of the rights that are
specifically granted under this License. You may not convey a covered
work if you are a party to an arrangement with a third party that is
in the business of distributing software, under which you make payment
to the third party based on the extent of your activity of conveying
the work, and under which the third party grants, to any of the
parties who would receive the covered work from you, a discriminatory
patent license (a) in connection with copies of the covered work
conveyed by you (or copies made from those copies), or (b) primarily
for and in connection with specific products or compilations that
contain the covered work, unless you entered into that arrangement,
or
that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting
any implied license or other defenses to infringement that may
otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or
otherwise) that contradict the conditions of this License, they do not
excuse you from the conditions of this License. If you cannot convey a
covered work so as to satisfy simultaneously your obligations under this
License and any other pertinent obligations, then as a consequence you may

not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS"

WITHOUT WARRANTY
OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17.
Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by

the Free Software Foundation, either version 3 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>
This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what you want to
do, use the GNU Lesser General
Public License instead of this License. But first, please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.

1.33 coreutils 8.25

1.33.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies

of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer

can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand
ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees"
and
"recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically

linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered
by this License only if the output, given its
content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed;
section 10
makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention

is effected by exercising rights under this License with respect to
the covered work, and you disclaim any intention to limit operation or
modification of the work as a means of enforcing, against the work's
users, your or third parties' legal rights to forbid circumvention of
technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you
receive it, in any medium, provided that you conspicuously and
appropriately
publish on each copy an appropriate copyright notice;
keep intact all notices stating that this License and any
non-permissive terms added in accord with section 7 apply to the code;
keep intact all notices of the absence of any warranty; and give all
recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey,
and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to
produce it from the Program, in the form of source code under the
terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified
it, and giving a relevant date.

b) The work must carry prominent notices stating that it is
released under this License and any conditions added under section
7. This requirement modifies the requirement in section
4 to
"keep intact all notices".

c) You must license the entire work, as a whole, under this
License to anyone who comes into possession of a copy. This
License will therefore apply, along with any applicable section 7
additional terms, to the whole of the work, and all its parts,
regardless of how they are packaged. This License gives no
permission to license the work in any other way, but it does not
invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display
Appropriate Legal Notices; however, if the Program has interactive
interfaces that do not display Appropriate Legal Notices, your
work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to

copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install

modified object code on the User Product (for example, the work has been installed in
ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the
entire Program shall
be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or
limiting liability differently from the
terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or
requiring that modified versions of such material be marked in
reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or
authors of the material; or

e) Declining to grant rights under trademark law for use of some
trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that
material by anyone who conveys the material (or modified versions of
it) with contractual assumptions of liability to the recipient, for
any liability that these contractual assumptions directly impose on

those licensors and authors.

All other non-permissive additional terms are considered "further
restrictions" within the meaning of section 10. If the Program as you
received it, or any part of it, contains a notice stating that it is
governed by this License along with a term that is a further
restriction, you may remove that term. If a license document contains
a further restriction but permits relicensing or conveying under this
License, you may add to a covered work material governed by the terms
of that license document, provided that the further restriction does
not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you
must place, in the relevant source files, a statement of the
additional terms that apply to those files, or a notice indicating
where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the
form of a separately written license, or stated as exceptions;
the above
requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly
provided under this License. Any attempt otherwise to propagate or
modify it is void, and will automatically terminate your rights under
this License (including any patent licenses granted under the third
paragraph of section 11).

However, if you cease all violation of this License, then your
license from a particular copyright holder is reinstated (a)

provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright
holder, and you cure the violation prior to 30 days after
your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights
granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For
purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this
License, through a
publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have

actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17.
Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>
This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what you want to
do, use the GNU Lesser General
Public License instead of this License. But first, please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.

1.34 cpio 2.12

1.34.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for
software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses
are designed to make sure that you
have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer
you this License
giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we

stand ready to extend this provision to those domains
in future versions
of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To
"modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate

Legal Notices"
to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than
the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing
those activities but
which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding

Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content,
constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users'
Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep
intact all notices stating that this License and any
non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license
the entire work, as a whole, under this
License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and

its resulting copyright are not
used to limit the access or legal rights of the compilation's users
beyond what the individual works permit. Inclusion of a covered work
in an aggregate does not cause this License to apply to the other
parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms
of sections 4 and 5, provided that you also convey the
machine-readable Corresponding Source under the terms of this License,
in one of these ways:

a) Convey the object code in, or embodied in, a physical product
(including a physical distribution medium), accompanied by the
Corresponding Source fixed on a durable physical medium
customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product
(including a physical distribution medium), accompanied by a
written offer, valid for at least three years and valid for as
long as you offer spare parts or customer
support for that product
model, to give anyone who possesses the object code either (1) a
copy of the Corresponding Source for all the software in the
product that is covered by this License, on a durable physical
medium customarily used for software interchange, for a price no
more than your reasonable cost of physically performing this
conveying of source, or (2) access to copy the
Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the
written offer to provide the Corresponding Source. This
alternative is allowed only occasionally and noncommercially, and
only if you received the object code with such an offer, in accord
with subsection 6b.

d) Convey the object code by offering access from a designated
place (gratis or for a charge), and offer equivalent access to the
Corresponding Source in the same way through the same place at no
further charge.
You need not require recipients to copy the
Corresponding Source along with the object code. If the place to
copy the object code is a network server, the Corresponding Source
may be on a different server (operated by you or a third party)
that supports equivalent copying facilities, provided you maintain
clear directions next to the object code saying where to find the
Corresponding Source. Regardless of what server hosts the

Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object
code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute
modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information

does not include a
requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included
in this License, to the extent
that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections
15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your
receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time
you convey a covered work, the recipient automatically
receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not

impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that

country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed

under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING
WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS
THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY
GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE
USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF
DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD
PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS),
EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF
SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer
of warranty and limitation of liability provided
above cannot be given local legal effect according to their terms,
reviewing courts shall apply local law that most closely approximates
an absolute waiver of all civil liability in connection with the
Program, unless a warranty or assumption of liability accompanies a
copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest
possible use to the public, the best way to achieve this is to make it
free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest
to attach them to the start of each source file to most effectively
state the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief
idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation, either version 3 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License

along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>
This program comes with
ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what you want to do, use the GNU Lesser General
Public License instead of this License. But first,
please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.

1.35 e2fsprogs 1.43

1.35.1 Available under license :

This package was added to the e2fsprogs debian source package by
Theodore Ts'o <tytso@mit.edu> on Sat Mar 15 15:33:37 EST 2003

It is part of the main e2fsprogs distribution, which can be found at:

http://sourceforge.net/projects/e2fsprogs

Upstream Author: Theodore Ts'o <tytso@mit.edu>

Copyright:

Copyright (C) 1999, 2001 by Andries Brouwer
Copyright (C) 1999, 2000, 2003 by Theodore Ts'o

You are free to distribute this software under the terms of the GNU
Lesser (Library) General Public License.

On Debian systems, the complete text of the GNU Lesser (Library)
General Public License can be found in /usr/share/common-licenses/LGPL-2.
This is the Debian GNU/Linux prepackaged version of the static EXT2
file system consistency checker (e2fsck.static). The EXT2 utilities
were written by Theodore Ts'o <tytso@mit.edu> and Remy Card
<card@masi.ibp.fr>.

Sources were obtained from http://sourceforge.net/projects/e2fsprogs

Packaging is Copyright (c) 2003-2006 Theodore Ts'o <tytso@mit.edu>
        Copyright (c) 1997-2003 Yann Dirson <dirson@debian.org>
    Copyright (c) 2001 Alcove <http://www.alcove.com/>
    Copyright (c) 1997 Klee Dienes
    Copyright (c) 1995-1996 Michael Nonweiler <mrn20@cam.ac.uk>

Upstream Author: Theodore Ts'o <tytso@mit.edu>

Copyright notice:

This package, the EXT2 filesystem utilities, is protected by the GNU
General Public License.

 Copyright (c) 1993, 1994, 1995, 1996, 1997, 1998, 1999, 2000,
 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008 by Theodore Ts'o

On Debian GNU systems, the complete text of the GNU General
Public License can be found in `/usr/share/common-licenses/GPL-2'.
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
  notice, and the entire permission notice in its entirety,
  including the disclaimer of warranties.
2. Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote
  products derived from this software without specific prior
  written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ALL OF
WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE
LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR

CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT
OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
USE OF THIS SOFTWARE, EVEN IF NOT ADVISED OF THE POSSIBILITY OF SUCH
DAMAGE.
This is the Debian GNU/Linux prepackaged version of the translation
files of the EXT2 file system utilities. The EXT2 utilities were
written by Theodore Ts'o <tytso@mit.edu> and Remy Card
<card@masi.ibp.fr>.

Sources were obtained from http://sourceforge.net/projects/e2fsprogs

Packaging is Copyright (c) 2003-2006 Theodore Ts'o <tytso@mit.edu>
Copyright (c) 1997-2003 Yann Dirson <dirson@debian.org>
Copyright (c) 2001 Alcove <http://www.alcove.com/>
Copyright (c) 1997 Klee Dienes
Copyright (c) 1995-1996 Michael Nonweiler <mrn20@cam.ac.uk>

Upstream Author: Theodore Ts'o <tytso@mit.edu>

Copyright notice:

This package, the EXT2 filesystem utilities, is protected by the GNU
General Public License.

Copyright (c) 1993, 1994, 1995, 1996, 1997, 1998, 1999, 2000,
2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008 by Theodore Ts'o

On Debian GNU systems, the complete text of the GNU General
Public License can be found in `/usr/share/common-licenses/GPL-2'.
This package was added to the e2fsprogs debian source package by
Theodore Ts'o <tytso@mit.edu> on Fri Dec 14 22:24:35 EST 2007

It is part of the main e2fsprogs distribution, which can be found at:

http://sourceforge.net/projects/e2fsprogs

Upstream Author: Theodore Ts'o <tytso@mit.edu>

Copyright:

Copyright (C) 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007 by
Theodore Ts'o

Redistribution and use in source and binary forms, with or without

modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
  notice, and the entire permission notice in its entirety,
  including the disclaimer of warranties.
2. Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote
  products derived from
 this software without specific prior
  written permission.

THIS SOFTWARE IS PROVIDED ``AS IS" AND ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ALL OF
WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE
LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT
OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
USE OF THIS SOFTWARE, EVEN IF NOT ADVISED OF THE POSSIBILITY OF SUCH
DAMAGE.
/*

Copyright 1987 by the Student Information Processing Board
 of the Massachusetts Institute of Technology

Permission to use, copy, modify, and distribute this software
and its documentation for any purpose and without fee is
hereby granted, provided that the above copyright notice
appear in all copies and that both that copyright notice and
this permission notice appear in supporting documentation,
and that the names of M.I.T. and the M.I.T. S.I.P.B. not be
used in advertising or publicity pertaining to distribution
of the software without specific, written prior permission.
M.I.T. and the M.I.T. S.I.P.B. make no representations about
the suitability of this software for any purpose. It is
provided "as is" without express or implied warranty.

*/
Index: tdbsa/tdb.c
===
--- tdbsa.orig/tdb.c
+++ tdbsa/tdb.c
@@ -4,11 +4,11 @@ Rev: 23371

Last Changed Date: 2007-06-06 20:14:06 -0400 (Wed, 06 Jun 2007)
*/
 /*
- Unix SMB/CIFS implementation.
+ trivial database library - standalone version

- trivial database library - private includes
-
- Copyright (C) Andrew Tridgell 2005
+ Copyright (C) Andrew Tridgell 1999-2005
+ Copyright (C) Jeremy Allison 2000-2006
+ Copyright (C) Paul `Rusty' Russell 2000

** NOTE! The following LGPL license applies to the tdb
** library. This does NOT imply that all of Samba is released
EXT2ED is hereby placed under the terms of the GNU General Public License.
Follows the GNU license.

Gadi Oxman, August 1995

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
675 Mass Ave, Cambridge, MA 02139, USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it. (Some other Free Software Foundation software is covered by
the
GNU Library General Public License instead.) You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price. Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it

in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents
constitute a work based on the
Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You
must cause the modified files to carry prominent notices
stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program
is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in

themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or
with a work based on the Program) on a volume of
a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information
you received as to the offer
to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the

operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access
to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program
(or any work based on the
Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously
your obligations under this
License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to

refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to
the wide range of software distributed
through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will
be
similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes

make exceptions for this. Our decision will be guided by the two goals
of preserving the free status of all derivatives of our free software and
of promoting
the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY
TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED
TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Appendix: How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) 19yy <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19yy name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY;
for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider
it more useful to permit linking proprietary applications with the
library. If this is what you want to do, use the GNU Library General
Public License instead of this License.
This package, the EXT2 filesystem utilities, are made available under
the GNU Public License version 2, with the exception of the lib/ext2fs
and lib/e2p libraries, which are made available under the GNU Library
General Public License Version 2, the lib/uuid library which is made
available under a BSD-style license and the lib/et and lib/ss
libraries which are made available under an MIT-style license. Please

see lib/uuid/COPYING for more details for the license for the files
comprising the libuuid library, and the source file headers of the
libet and libss libraries for more information.

The most recent officially distributed version can be found at
http://e2fsprogs.sourceforge.net. If you need to make a distribution,
that's the one you should use. If there is some reason why you'd like
a more recent version that is still in ALPHA testing (i.e., either
using the "WIP" test distributions or one from the hg or git
repository from the development branch, please contact me
(tytso@mit.edu)
before you ship. The release schedules for this
package are flexible, if you give me enough lead time.

Theodore Ts'o
23-June-2007

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it. (Some other Free Software Foundation software
is covered by
the GNU Library General Public License instead.) You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price. Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source
code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms
and conditions for copying, distribution and
modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of

running the Program is not restricted, and the output from the Program is covered
only if its contents constitute a work based on the
Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on
the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based

on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with
the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it
with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made
by offering
access to copy from a designated place, then offering equivalent
access to copy the source code from the same place counts as
distribution of the source code, even though third parties are not
compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program
except as expressly provided under this License. Any attempt
otherwise to copy, modify, sublicense or distribute the Program is
void, and will automatically terminate your rights under this License.
However, parties who have received copies, or rights, from you under
this License will not have their licenses terminated so long as such
parties remain in full compliance.

5. You are not required to accept this License, since you have not
signed it. However, nothing else grants you permission to modify or
distribute the Program or its derivative works. These actions are
prohibited by law if you do not accept this License. Therefore, by
modifying or distributing
the Program (or any work based on the
Program), you indicate your acceptance of this License to do so, and
all its terms and conditions for copying, distributing or modifying
the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the
Program), the recipient automatically receives a license from the
original licensor to copy, distribute or modify the Program subject to
these terms and conditions. You may not impose any further
restrictions on the recipients' exercise of the rights granted herein.
You are not responsible for enforcing compliance by third parties to
this License.

7. If, as a consequence of a court judgment or allegation of patent
infringement or for any other reason (not limited to patent issues),
conditions are imposed on you (whether by court order, agreement or
otherwise) that contradict the conditions of this License, they do not
excuse you from the conditions of this License. If you cannot
distribute so as to satisfy
simultaneously your obligations under this
License and any other pertinent obligations, then as a consequence you
may not distribute the Program at all. For example, if a patent
license would not permit royalty-free redistribution of the Program by
all those who receive copies directly or indirectly through you, then
the only way you could satisfy both it and this License would be to
refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under

any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous
contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such
new versions will
be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software

and
of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE
USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name
of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision
comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a
subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this is what you want to do, use the GNU Library General
Public License instead of this License.

GNU LIBRARY GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the library GPL. It is
numbered 2 because it goes with version 2 of the ordinary GPL.]

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
Licenses are intended to guarantee your freedom to share and change
free software--to make sure the software is free for
all its users.

This license, the Library General Public License, applies to some
specially designated Free Software Foundation software, and to any
other libraries whose authors decide to use it. You can use it for
your libraries, too.

When we speak of free software, we are referring to freedom, not
price. Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid
anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate to certain responsibilities for you if
you distribute copies of the library, or if you modify it.

For example, if you distribute copies of the library, whether gratis
or for a
fee, you must give the recipients all the rights that we gave
you. You must make sure that they, too, receive or can get the source
code. If you link a program with the library, you must provide
complete object files to the recipients so that they can relink them
with the library, after making changes to the library and recompiling
it. And you must show them these terms so they know their rights.

Our method of protecting your rights has two steps: (1) copyright
the library, and (2) offer you this license which gives you legal
permission to copy, distribute and/or modify the library.

Also, for each distributor's protection, we want to make certain
that everyone understands that there is no warranty for this free

library. If the library is modified by someone else and passed on, we
want its recipients to know that what they have is not the original
version, so that any problems introduced by others will not reflect on
the original authors' reputations.

Finally, any free program
is threatened constantly by software
patents. We wish to avoid the danger that companies distributing free
software will individually obtain patent licenses, thus in effect
transforming the program into proprietary software. To prevent this,
we have made it clear that any patent must be licensed for everyone's
free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary
GNU General Public License, which was designed for utility programs. This
license, the GNU Library General Public License, applies to certain
designated libraries. This license is quite different from the ordinary
one; be sure to read it in full, and don't assume that anything in it is
the same as in the ordinary license.

The reason we have a separate public license for some libraries is that
they blur the distinction we usually make between modifying or adding to a
program and simply using it. Linking a program with a library, without
changing the library, is
in some sense simply using the library, and is
analogous to running a utility program or application program. However, in
a textual and legal sense, the linked executable is a combined work, a
derivative of the original library, and the ordinary General Public License
treats it as such.

Because of this blurred distinction, using the ordinary General
Public License for libraries did not effectively promote software
sharing, because most developers did not use the libraries. We
concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the
users of those programs of all benefit from the free status of the
libraries themselves. This Library General Public License is intended to
permit developers of non-free programs to use free libraries, while
preserving your freedom as a user of such programs to change the free
libraries that are incorporated in them. (We have not seen how to achieve
this as regards changes in
header files, but we have achieved it as regards
changes in the actual functions of the Library.) The hope is that this
will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and
modification follow. Pay close attention to the difference between a

"work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

GNU LIBRARY GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called "this License"). Each licensee is addressed
as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities
other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact

all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each

and every part regardless of who wrote
it.

Thus, it is not the intent of this section to claim rights or contest
your rights to work written entirely by you; rather, the intent is to
exercise the right to control the distribution of derivative or
collective works based on the Library.

In addition, mere aggregation of another work not based on the Library
with the Library (or with a work based on the Library) on a volume of
a storage or distribution medium does not bring the other work under
the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public
License instead of this License to a given copy of the Library. To do
this, you must alter all the notices that refer to this License, so
that they refer to the ordinary GNU General Public License, version 2,
instead of to this License. (If a newer version than version 2 of the
ordinary GNU General Public License has appeared, then you can specify
that version instead if you wish.) Do not make
any other change in
these notices.

Once this change is made in a given copy, it is irreversible for
that copy, so the ordinary GNU General Public License applies to all
subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of
the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or
derivative of it, under Section 2) in object code or executable form
under the terms of Sections 1 and 2 above provided that you accompany
it with the complete corresponding machine-readable source code, which
must be distributed under the terms of Sections 1 and 2 above on a
medium customarily used for software interchange.

If distribution of object code is made by offering access to copy
from a designated place, then offering equivalent access to copy the
source code from the same place satisfies the requirement to
distribute the source code, even though third parties are not
compelled
to copy the source along with the object code.

5. A program that contains no derivative of any portion of the
Library, but is designed to work with the Library by being compiled or
linked with it, is called a "work that uses the Library". Such a
work, in isolation, is not a derivative work of the Library, and

therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library,
or if the work is itself a library. The
threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also compile or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that
the terms permit
modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked

with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

c) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

d) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the

Sections above.

b) Give prominent notice with the combined library of the fact
that part of it is a work based on the Library, and explaining
where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute
the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement
or
otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply,

and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Library General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY
AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them
to the start of each source file to most effectively
convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or
modify it under the terms of the GNU Library General Public
License as published by the Free Software Foundation; either
version 2 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
Library General Public License for more details.

You should have received a copy of the GNU Library General Public
License along with this library; if not, write to the Free Software
Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the library, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the
library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!
This is the Debian GNU/Linux prepackaged version of the EXT2 file
system utilities (e2fsck, mke2fs, etc.). The EXT2 utilities were
written by Theodore Ts'o <tytso@mit.edu> and Remy Card <card@masi.ibp.fr>.

Sources were obtained from http://sourceforge.net/projects/e2fsprogs

Packaging is Copyright (c) 2003-2007 Theodore Ts'o <tytso@mit.edu>
Copyright (c) 1997-2003 Yann Dirson <dirson@debian.org>
Copyright (c) 2001 Alcove <http://www.alcove.com/>
Copyright (c) 1997 Klee Dienes
Copyright (c) 1995-1996 Michael Nonweiler <mrn20@cam.ac.uk>

Upstream Author: Theodore Ts'o <tytso@mit.edu>

Copyright notice:

This package, the EXT2 filesystem utilities, are made available under
the GNU General Public License version 2, with the exception of the
lib/ext2fs and lib/e2p libraries, which are made available under the
GNU Library General Public License Version 2, the lib/uuid library
which is made available under a BSD-style license and the lib/et and
lib/ss libraries
which are made available under an MIT-style license.

Copyright (c) 1993, 1994, 1995, 1996, 1997, 1998, 1999, 2000,
2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008 by Theodore Ts'o

On Debian GNU systems, the complete text of the GNU General Public
License can be found in `/usr/share/common-licenses/GPL-2'. The
complete text of the GNU Library General Public License can be found
in '/usr/share/common-licenses/LGPL-2'.

The license used for lib/et and lib/ss libraries is:

Copyright 1987 by the Student Information Processing Board
of the Massachusetts Institute of Technology

Permission to use, copy, modify, and distribute this software and
its documentation for any purpose is hereby granted, provided that
the names of M.I.T. and the M.I.T. S.I.P.B. not be used in
advertising or publicity pertaining to distribution of the software
without specific, written prior permission. M.I.T. and the
M.I.T. S.I.P.B. make no representations about the suitability of
this
software for any purpose. It is provided "as is" without
express or implied warranty.

The license used for lib/uuid is:

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
notice, and the entire permission notice in its entirety,
including the disclaimer of warranties.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote
products derived from this software without specific prior
written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
OF MERCHANTABILITY AND
FITNESS FOR A PARTICULAR PURPOSE, ALL OF
WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE
LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT
OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF

LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
USE OF THIS SOFTWARE, EVEN IF NOT ADVISED OF THE POSSIBILITY OF SUCH
DAMAGE.
This package was added to the e2fsprogs debian source package by
Theodore Ts'o <tytso@mit.edu> on Sat Mar 15 15:33:37 EST 2003

It is part of the main e2fsprogs distribution, which can be found at:

http://sourceforge.net/projects/e2fsprogs

Upstream Author: Theodore Ts'o <tytso@mit.edu>

Copyright:

Copyright (C) 1999, 2000, 2003, 2004 by Theodore Ts'o

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
notice, and the entire permission notice in its entirety,
including the disclaimer of warranties.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote
products derived from this software without specific
prior
written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ALL OF
WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE
LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT
OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
USE OF THIS SOFTWARE, EVEN IF NOT ADVISED OF THE POSSIBILITY OF SUCH
DAMAGE.
#
This is a Makefile stub which handles the creation of BSD shared
libraries.
#
In order to use this stub, the following makefile variables must be defined.

```
#
# BSDLIB_VERSION = 1.0
# BSDLIB_IMAGE = libce
# BSDLIB_MYDIR = et
# BSDLIB_INSTALL_DIR = $(SHLIBDIR)
#

all:: image

real-subdirs:: Makefile
 @echo " MKDIR pic"
 @mkdir -p pic

BSD_LIB = $(BSDLIB_IMAGE).so.$(BSDLIB_VERSION)
BSDLIB_PIC_FLAG = -fpic

image:  $(BSD_LIB)

$(BSD_LIB): $(OBJS)
 (cd pic; ld -Bshareable -o $(BSD_LIB) $(LDFLAGS_SHLIB) $(OBJS))
 $(MV) pic/$(BSD_LIB) .
 $(RM) -f ../$(BSD_LIB)
 (cd ..; $(LN) $(LINK_BUILD_FLAGS) \
  `echo $(my_dir) | sed -e 's;lib/;;'`/$(BSD_LIB) $(BSD_LIB))

install-shlibs install:: $(BSD_LIB)
 @echo " INSTALL_PROGRAM $(BSDLIB_INSTALL_DIR)/$(BSD_LIB)"
 @$(INSTALL_PROGRAM) $(BSD_LIB) \
  $(DESTDIR)$(BSDLIB_INSTALL_DIR)/$(BSD_LIB)
 @-$(LDCONFIG)

install-strip: install

install-shlibs-strip: install-shlibs

uninstall-shlibs uninstall::
 $(RM) -f $(DESTDIR)$(BSDLIB_INSTALL_DIR)/$(BSD_LIB)

clean::
 $(RM)
 -rf pic
 $(RM) -f $(BSD_LIB)
 $(RM) -f ../$(BSD_LIB)
This is the Debian GNU/Linux prepackaged version of the ss
command-line interface parsing library. It is currently
distributed together with the EXT2 file system utilities, which are
otherwise packaged as "e2fsprogs".
```

This package was put together by Yann Dirson <dirson@debian.org>,
from sources obtained from a mirror of:
tsx-11.mit.edu:/pub/linux/packages/ext2fs/

From the original distribution:

Copyright 1987, 1988 by the Student Information Processing Board
 of the Massachusetts Institute of Technology

Permission to use, copy, modify, and distribute this software
and its documentation for any purpose and without fee is
hereby granted, provided that the above copyright notice
appear in all copies and that both that copyright notice and
this permission notice appear in supporting documentation,
and that the names of M.I.T. and the M.I.T. S.I.P.B. not be
used in advertising or publicity pertaining to distribution
of the software without specific, written prior permission.
M.I.T. and
 the M.I.T. S.I.P.B. make no representations about
the suitability of this software for any purpose. It is
provided "as is" without express or implied warranty.
This is the Debian GNU/Linux prepackaged version of the Common Error
Description library. It is currently distributed together with the EXT2 file
system utilities, which are otherwise packaged as "e2fsprogs".

This package was put together by Yann Dirson <dirson@debian.org>,
from sources obtained from a mirror of:
tsx-11.mit.edu:/pub/linux/packages/ext2fs/

From the original distribution:

Copyright 1987, 1988 by the Student Information Processing Board
 of the Massachusetts Institute of Technology

Permission to use, copy, modify, and distribute this software
and its documentation for any purpose and without fee is
hereby granted, provided that the above copyright notice
appear in all copies and that both that copyright notice and
this permission notice appear in supporting documentation,
and that the names of M.I.T. and the M.I.T. S.I.P.B. not be
used in advertising or publicity pertaining to distribution
of the software without specific, written prior permission.
M.I.T. and the M.I.T.
 S.I.P.B. make no representations about
the suitability of this software for any purpose. It is
provided "as is" without express or implied warranty.

1.36 patch 2.7.5

1.36.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for
software and other kinds of works.

The licenses for most software and other practical works are designed
to take away your freedom to share and change the works. By contrast,
the GNU General Public License is intended to guarantee your freedom to
share and change all versions of a program--to make sure it remains free
software for all its users. We, the Free Software Foundation, use the
GNU General Public License for most of our software; it applies also to
any other work released this way by its authors. You can apply it to
your programs, too.

When we speak of free software, we are referring to
freedom, not
price. Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
them if you wish), that you receive source code or can get it if you
want it, that you can change the software or use pieces of it in new
free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you
these rights or asking you to surrender the rights. Therefore, you have
certain responsibilities if you distribute copies of the software, or if
you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether
gratis or for a fee, you must pass on to the recipients the same
freedoms that you received. You must make sure that they, too, receive
or can get the source code. And you must show them these terms so they
know their rights.

Developers that use the GNU GPL protect your rights with two steps:
(1)
assert copyright on the software, and (2) offer you this License
giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand
ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees"
and
"recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all

the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately
publish on each copy an appropriate copyright notice;
keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts,

regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and

only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in
the same way through the same place at no
further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source
as a System Library, need not be
included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization
keys, or other information required to install
and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in
ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the
entire Program shall
be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of

that material) supplement the terms of this License with terms:

a) Disclaiming warranty or
limiting liability differently from the
terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or
author attributions in that material or in the Appropriate Legal
Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or
requiring that modified versions of such material be marked in
reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or
authors of the material; or

e) Declining to grant rights under trademark law for use of some
trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that
material by anyone who conveys the material (or modified versions of
it) with contractual assumptions of liability to the recipient, for
any liability that these contractual assumptions directly impose on

those licensors and authors.

All other non-permissive additional terms are considered "further
restrictions" within the meaning of section 10. If the Program as you
received it, or any part of it, contains a notice stating that it is
governed by this License along with a term that is a further
restriction, you may remove that term. If a license document contains
a further restriction but permits relicensing or conveying under this
License, you may add to a covered work material governed by the terms
of that license document, provided that the further restriction does
not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you
must place, in the relevant source files, a statement of the
additional terms that apply to those files, or a notice indicating
where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the
form of a separately written license, or stated as exceptions;
the above
requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright
holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an

organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights
granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For
purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license,

and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a

covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY

APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS"
WITHOUT WARRANTY
OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17.
Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where
the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation, either version 3 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>
This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what you want to
do, use the GNU Lesser General
Public License instead of this License. But first, please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.

1.37 ebtables 2.0.10

1.37.1 Available under license :

All code in this package, including the code from the extensions,
is released under the GPL license, which you find hereafter.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
675 Mass Ave, Cambridge, MA 02139, USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your
programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your
rights with two steps: (1) copyright the software, and
(2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so

that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1

above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that
you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply
to the modified work as a whole. If
identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution
medium does not bring the other work under
the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by

modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in
certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Program under this License
may add an explicit geographical distribution limitation excluding
those countries, so that distribution is permitted only in or among
countries not thus excluded. In such case, this License incorporates
the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions
of the General Public License from time to time. Such new versions will
be similar in spirit to the present version, but may differ in detail to
address
new problems or concerns.

Each version is given a distinguishing version number. If the Program
specifies a version number of this License which applies to it and "any
later version", you have the option of following the terms and conditions
either of that version or of any later version published by the Free
Software Foundation. If the Program does not specify a version number of
this License, you may choose any version ever published by the Free Software
Foundation.

10. If you wish to incorporate parts of the Program into other free
programs whose distribution conditions are different, write to the author
to ask for permission. For software which is copyrighted by the Free
Software Foundation, write to the Free Software Foundation; we sometimes
make exceptions for this. Our decision will be guided by the two goals
of preserving the free status of all derivatives of our free software and
of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY
FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES
PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED
OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS
TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE
PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING,
REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING
WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR
REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES,
INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING
OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED

TO LOSS OF DATA OR DATA BEING
RENDERED INACCURATE OR LOSSES SUSTAINED BY
YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER
PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE
POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Appendix: How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest
possible use to the public, the best way to achieve this is to make it
free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest
to attach them to the start of each source file to most effectively
convey the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) 19yy <name of author>

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation; either version 2 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19yy name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome
to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate

parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

 Yoyodyne, Inc., hereby disclaims all copyright interest in the program
 `Gnomovision' (which makes passes at compilers) written by James Hacker.

 <signature of Ty Coon>, 1 April 1989
 Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library.
  If this is what you want to do, use the GNU Library General
Public License instead of this License.

1.38 libevent 2.1.8

1.38.1 Available under license :

Libevent is available for use under the following license, commonly known
as the 3-clause (or "modified") BSD license:

==============================
Copyright (c) 2000-2007 Niels Provos <provos@citi.umich.edu>
Copyright (c) 2007-2012 Niels Provos and Nick Mathewson

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
  notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products
  derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING,
 BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT,

INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
==========

Portions of Libevent are based on works by others, also made available by
them under the three-clause BSD license above. The copyright notices are
available in the corresponding source files; the license is as above. Here's
a list:

log.c:
Copyright (c) 2000 Dug Song <dugsong@monkey.org>
Copyright (c) 1993 The Regents of the University of California.

strlcpy.c:
Copyright (c) 1998 Todd C. Miller <Todd.Miller@courtesan.com>

win32select.c:
Copyright (c) 2003 Michael A. Davis <mike@datanerds.net>

evport.c:
Copyright (c) 2007 Sun Microsystems

ht-internal.h:
Copyright (c) 2002 Christopher Clark

minheap-internal.h:
Copyright (c) 2006 Maxim Yegorushkin <maxim.yegorushkin@gmail.com>

==========

The arc4module is available under the following, sometimes called the
"OpenBSD" license:

Copyright (c) 1996, David Mazieres <dm@uun.org>
Copyright (c) 2008, Damien Miller <djm@openbsd.org>

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES
WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR

BE LIABLE FOR
ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

==========

The Windows timer code is based on code from libutp, which is
distributed under this license, sometimes called the "MIT" license.

Copyright (c) 2010 BitTorrent, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be
included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
CMake - Cross Platform Makefile Generator
Copyright 2000-2013 Kitware, Inc.
Copyright 2000-2011 Insight Software Consortium
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

* Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

* Neither the names of Kitware, Inc., the Insight Software Consortium,
 nor the names of their contributors may be used to endorse or promote
 products derived from this software without specific prior written
 permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO,
 THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT
HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The above copyright and license notice applies to distributions of
CMake in source and binary form. Some source files contain additional
notices of original copyright by their contributors; see each source
for details. Third-party software packages supplied with CMake under
compatible licenses provide their
 own copyright notices documented in
corresponding subdirectories.

CMake was initially developed by Kitware with the following sponsorship:

* National Library of Medicine at the National Institutes of Health
  as part of the Insight Segmentation and Registration Toolkit (ITK).

* US National Labs (Los Alamos, Livermore, Sandia) ASC Parallel
  Visualization Initiative.

* National Alliance for Medical Image Computing (NAMIC) is funded by the
  National Institutes of Health through the NIH Roadmap for Medical Research,
  Grant U54 EB005149.

* Kitware, Inc.
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

1. Redistributions of source code must retain the copyright

notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products
derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
NOT LIMITED TO, PROCUREMENT
OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF
THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

1.39 libtirpc 1.0.1

1.39.1 Available under license :

/*
* Copyright (c) Copyright (c) Bull S.A. 2005 All Rights Reserved.
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the above copyright
*   notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*   notice, this list of conditions and the following disclaimer in the
*   documentation and/or other materials provided with the distribution.
* 3. The name of the author may not be used to endorse or promote products
*   derived from this software without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR
* IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
* OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
* IN NO EVENT SHALL THE AUTHOR BE LIABLE
 FOR ANY DIRECT, INDIRECT,
* INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
* DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
* THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
* (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF
* THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
*/

1.40 avahi 0.6.32

1.40.1 Available under license :

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts
as the successor of the GNU Library Public License, version 2, hence
the version number 2.1.]

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
Licenses are intended to guarantee your freedom to share and change
free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some
specially designated software packages--typically libraries--of the
Free Software Foundation and other authors who decide
to use it. You
can use it too, but we suggest you first think carefully about whether
this license or the ordinary General Public License is the better
strategy to use in any particular case, based on the explanations
below.

When we speak of free software, we are referring to freedom of use,
not price. Our General Public Licenses are designed to make sure that
you have the freedom to distribute copies of free software (and charge
for this service if you wish); that you receive source code or can get
it if you want it; that you can change the software and use pieces of
it in new free programs; and that you are informed that you can do
these things.

To protect your rights, we need to make restrictions that forbid
distributors to deny you these rights or to ask you to surrender these
rights. These restrictions translate to certain responsibilities for
you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages

are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under

copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a

table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be
reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary
GNU General Public
License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all

subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the

object code for the work under the terms of Section 6.
Any executables containing that work also fall under Section 6,
whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or
link a "work that uses the Library" with the Library to produce a
work containing portions of the Library, and distribute that work
under terms of your choice, provided that the terms permit
modification of the work for the customer's own use and reverse
engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the
Library is used in it and that the Library and its use are covered by
this License. You must supply a copy of this License. If the work
during execution displays copyright notices, you must include the
copyright notice for the Library among them, as well as a reference
directing the user to the copy of this License. Also, you must do one
of these things:

a) Accompany
the work with the complete corresponding
machine-readable source code for the Library including whatever
changes were used in the work (which must be distributed under
Sections 1 and 2 above); and, if the work is an executable linked
with the Library, with the complete machine-readable "work that
uses the Library", as object code and/or source code, so that the
user can modify the Library and then relink to produce a modified
executable containing the modified Library. (It is understood
that the user who changes the contents of definitions files in the
Library will not necessarily be able to recompile the application
to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the
Library. A suitable mechanism is one that (1) uses at run time a
copy of the library already present on the user's computer system,
rather than copying library functions into the executable, and (2)
will operate
properly with a modified version of the library, if
the user installs one, as long as the modified version is
interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least
three years, to give the same user the materials specified in
Subsection 6a, above, for a charge no more than the cost of
performing this distribution.

d) If distribution of the work is made by offering access to copy
from a designated place, offer equivalent access to copy the above

specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally
distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with
any other library
facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or

distribute the Library or its derivative works. These actions are prohibited by law
if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse
you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution
system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to

be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY

AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE,
BE LIABLE TO YOU
FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively
convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA
02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

1.41 i2c-tools 3.1

1.41.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed
to make sure that you
have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid

anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute
and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which
contains
a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program

is covered only if its contents constitute a work based on the
Program (independent of having been made by running the Program).
Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies
of the Program's
source code as you receive it, in any medium, provided that you
conspicuously and appropriately publish on each copy an appropriate
copyright notice and disclaimer of warranty; keep intact all the
notices that refer to this License and to the absence of any warranty;
and give any other recipients of the Program a copy of this License
along with the Program.

You may charge a fee for the physical act of transferring a copy, and
you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion
of it, thus forming a work based on the Program, and copy and
distribute such modifications or work under the terms of Section 1
above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices
stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in
whole
or in part contains or is derived from the Program or any
part thereof, to be licensed as a whole at no charge to all third
parties under the terms of this License.

c) If the modified program normally reads commands interactively
when run, you must cause it, when started running for such
interactive use in the most ordinary way, to print or display an
announcement including an appropriate copyright notice and a
notice that there is no warranty (or else, saying that you provide
a warranty) and that users may redistribute the program under
these conditions, and telling the user how to view a copy of this
License. (Exception: if the Program itself is interactive but
does not normally print such an announcement, your work based on
the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If
identifiable sections of that work are not derived from the Program,
and can be reasonably considered
independent and separate works in
themselves, then this License, and its terms, do not apply to those
sections when you distribute them as separate works. But when you
distribute the same sections as part of a whole which is a work based

on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it,
under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or
executable form with such
an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under

any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through
any other system and a licensee cannot
impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number
of this License which applies to it and "any
later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW.
EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN
IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License,
or
(at your option) any later version.

This program is distributed in the hope that it will be useful,

but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License along
with this program; if not, write to the Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w'
and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this is what you want to do, use the GNU Lesser General
Public License instead of this License.

1.42 parted 3.2

1.42.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for
software and other kinds of works.

The licenses for most software and other practical works are designed
to take away your freedom to share and change the works. By contrast,
the GNU General Public License is intended to guarantee your freedom to
share and change all versions of a program--to make sure it remains free
software for all its users. We, the Free Software Foundation, use the
GNU General Public License for most of our software; it applies also to
any other work released this way by its authors. You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price. Our General Public Licenses
are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
them if you wish), that you receive source code or can get it if you
want it, that you can change the software or use pieces of it in new
free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you
these rights or asking you to surrender the rights. Therefore, you have
certain responsibilities if you distribute copies of the software, or if
you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether
gratis or for a fee, you must pass on to the recipients the same
freedoms that you received. You must make sure that they, too, receive
or can get the source code. And you must show them these terms so they
know their rights.

Developers that use the GNU GPL protect your rights with two steps:
(1) assert copyright on the software, and (2) offer
you this License
giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains
that there is no warranty for this free software. For both users' and
authors' sake, the GPL requires that modified versions be marked as
changed, so that their problems will not be attributed erroneously to
authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying,

distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source

includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content,
constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal
Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your

work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge.

You need not require recipients to copy the
Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object
code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute
modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied

by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or

author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your
receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time
you convey a covered work, the recipient automatically
receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if

the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not
impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control"
includes the right to grant
patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other
readily accessible means,
then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner

consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License,
you have
permission to link or combine any covered work with a work licensed
under version 3 of the GNU Affero General Public License into a single
combined work, and to convey the resulting work. The terms of this
License will continue to apply to the part which is the covered work,
but the special requirements of the GNU Affero General Public License,
section 13, concerning interaction through a network will apply to the
combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of
the GNU General Public License from time to time. Such new versions will
be similar in spirit to the present version, but may differ in detail to
address new problems or concerns.

Each version is given a distinguishing version number. If the
Program specifies that a certain numbered version of the GNU General
Public License "or any later version" applies to it, you have the
option of following the terms and conditions either
of that numbered
version or of any later version published by the Free Software
Foundation. If the Program does not specify a version number of the
GNU General Public License, you may choose any version ever published
by the Free Software Foundation.

If the Program specifies that a proxy can decide which future
versions of the GNU General Public License can be used, that proxy's
public statement of acceptance of a version permanently authorizes you
to choose that version for the Program.

Later license versions may give you additional or different
permissions. However, no additional obligations are imposed on any
author or copyright holder as a result of your choosing to follow a
later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY
APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT
HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY
OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING,
BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM

IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of
warranty and limitation of liability provided
above cannot be given local legal effect according to their terms,
reviewing courts shall apply local law that most closely approximates
an absolute waiver of all civil liability in connection with the
Program, unless a warranty or assumption of liability accompanies a
copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest
possible use to the public, the best way to achieve this is to make it
free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest
to attach them to the start of each source file to most effectively
state the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea
of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation, either version 3 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,

but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>
This program comes with ABSOLUTELY
NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what you want to do, use the GNU Lesser General
Public License instead of this License. But first,
please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.
@c The GNU Free Documentation License.
@center Version 1.3, 3 November 2008

@c This file is intended to be included within another document,
@c hence no sectioning command or @node.

@display
Copyright @copyright{} 2000, 2001, 2002, 2007, 2008 Free Software Foundation, Inc.
@uref{http://fsf.org/}

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.
@end display

@enumerate 0
@item
PREAMBLE

The purpose of this License is to make a manual, textbook, or other
functional and useful document @dfn{free} in the sense of freedom: to
assure everyone the effective freedom to copy and redistribute it,
with or without modifying it, either commercially or noncommercially.
Secondarily, this License preserves for the author and publisher a way
to get credit for their work, while not being considered responsible
for modifications made by others.

This License is a kind of ``copyleft'', which means that derivative
works of the document
must themselves be free in the same sense. It
complements the GNU General Public License, which is a copyleft
license designed for free software.

We have designed this License in order to use it for manuals for free
software, because free software needs free documentation: a free
program should come with manuals providing the same freedoms that the
software does. But this License is not limited to software manuals;
it can be used for any textual work, regardless of subject matter or
whether it is published as a printed book. We recommend this License
principally for works whose purpose is instruction or reference.

@item
APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that
contains a notice placed by the copyright holder saying it can be
distributed under the terms of this License. Such a notice grants a
world-wide, royalty-free license, unlimited in duration, to use that
work under the conditions stated herein. The ``Document'', below,
refers
to any such manual or work. Any member of the public is a
licensee, and is addressed as ``you''. You accept the license if you
copy, modify or distribute the work in a way requiring permission
under copyright law.

A ``Modified Version'' of the Document means any work containing the
Document or a portion of it, either copied verbatim, or with
modifications and/or translated into another language.

A ``Secondary Section'' is a named appendix or a front-matter section
of the Document that deals exclusively with the relationship of the
publishers or authors of the Document to the Document's overall
subject (or to related matters) and contains nothing that could fall

directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The ``Invariant Sections'' are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The ``Cover Texts'' are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A ``Transparent'' copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not ``Transparent'' is called ``Opaque''.

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, La@TeX{} input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The ``Title Page'' means, for a printed book, the title page itself,
plus such following pages as are needed to hold, legibly, the material
this License requires to appear in the title page. For works in
formats which do not have any title page as such, ``Title Page'' means
the text near the most prominent appearance of the work's title,
preceding the beginning of the body of the text.

The ``publisher'' means any person or entity that distributes copies
of the Document to the public.

A section ``Entitled XYZ'' means a named subunit of the Document whose
title either is precisely XYZ or contains XYZ in parentheses following
text that translates XYZ in another language. (Here XYZ stands for a
specific section name mentioned below, such as ``Acknowledgements'',
``Dedications'', ``Endorsements'',
 or ``History''.)  To ``Preserve the Title''
of such a section when you modify the Document means that it remains a
section ``Entitled XYZ'' according to this definition.

The Document may include Warranty Disclaimers next to the notice which
states that this License applies to the Document. These Warranty
Disclaimers are considered to be included by reference in this
License, but only as regards disclaiming warranties: any other
implication that these Warranty Disclaimers may have is void and has
no effect on the meaning of this License.

@item
VERBATIM COPYING

You may copy and distribute the Document in any medium, either
commercially or noncommercially, provided that this License, the
copyright notices, and the license notice saying this License applies
to the Document are reproduced in all copies, and that you add no other
conditions whatsoever to those of this License. You may not use
technical measures to obstruct or control the reading or further
copying of the copies
 you make or distribute. However, you may accept
compensation in exchange for copies. If you distribute a large enough
number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and
you may publicly display copies.

@item
COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have

printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the
title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute
an
Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

@item
MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

@enumerate A
@item

Use in the Title Page (and on the covers, if any) a title distinct
from that of the Document, and from those of previous versions
(which should, if there were any, be listed in the History section
of the Document). You may use the same
title as a previous version
if the original publisher of that version gives permission.

@item
List on the Title Page, as authors, one or more persons or entities
responsible for authorship of the modifications in the Modified
Version, together with at least five of the principal authors of the
Document (all of its principal authors, if it has fewer than five),
unless they release you from this requirement.

@item
State on the Title page the name of the publisher of the
Modified Version, as the publisher.

@item
Preserve all the copyright notices of the Document.

@item
Add an appropriate copyright notice for your modifications
adjacent to the other copyright notices.

@item
Include, immediately after the copyright notices, a license notice
giving the public permission to use the Modified Version under the
terms of this License, in the form shown in the Addendum below.

@item
Preserve in that license notice the full lists of Invariant Sections
and required Cover Texts given in the Document's
license notice.

@item
Include an unaltered copy of this License.

@item
Preserve the section Entitled ``History'', Preserve its Title, and add
to it an item stating at least the title, year, new authors, and
publisher of the Modified Version as given on the Title Page. If
there is no section Entitled ``History'' in the Document, create one
stating the title, year, authors, and publisher of the Document as
given on its Title Page, then add an item describing the Modified
Version as stated in the previous sentence.

@item

Preserve the network location, if any, given in the Document for
public access to a Transparent copy of the Document, and likewise
the network locations given in the Document for previous versions
it was based on. These may be placed in the ``History'' section.
You may omit a network location for a work that was published at
least four years before the Document itself, or if the original
publisher of the version it refers to gives permission.

@item
For any
 section Entitled ``Acknowledgements'' or ``Dedications'', Preserve
the Title of the section, and preserve in the section all the
substance and tone of each of the contributor acknowledgements and/or
dedications given therein.

@item
Preserve all the Invariant Sections of the Document,
unaltered in their text and in their titles. Section numbers
or the equivalent are not considered part of the section titles.

@item
Delete any section Entitled ``Endorsements''. Such a section
may not be included in the Modified Version.

@item
Do not retitle any existing section to be Entitled ``Endorsements'' or
to conflict in title with any Invariant Section.

@item
Preserve any Warranty Disclaimers.
@end enumerate

If the Modified Version includes new front-matter sections or
appendices that qualify as Secondary Sections and contain no material
copied from the Document, you may at your option designate some or all
of these sections as invariant. To do this, add their titles to the
list of Invariant
 Sections in the Modified Version's license notice.
These titles must be distinct from any other section titles.

You may add a section Entitled ``Endorsements'', provided it contains
nothing but endorsements of your Modified Version by various
parties---for example, statements of peer review or that the text has
been approved by an organization as the authoritative definition of a
standard.

You may add a passage of up to five words as a Front-Cover Text, and a
passage of up to 25 words as a Back-Cover Text, to the end of the list

of Cover Texts in the Modified Version. Only one passage of
Front-Cover Text and one of Back-Cover Text may be added by (or
through arrangements made by) any one entity. If the Document already
includes a cover text for the same cover, previously added by you or
by arrangement made by the same entity you are acting on behalf of,
you may not add another; but you may replace the old one, on explicit
permission from the previous publisher that added the old
one.

The author(s) and publisher(s) of the Document do not by this License
give permission to use their names for publicity for or to assert or
imply endorsement of any Modified Version.

@item
COMBINING DOCUMENTS

You may combine the Document with other documents released under this
License, under the terms defined in section 4 above for modified
versions, provided that you include in the combination all of the
Invariant Sections of all of the original documents, unmodified, and
list them all as Invariant Sections of your combined work in its
license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and
multiple identical Invariant Sections may be replaced with a single
copy. If there are multiple Invariant Sections with the same name but
different contents, make the title of each such section unique by
adding at the end of it, in parentheses, the name of the original
author or publisher of that section if known,
or else a unique number.
Make the same adjustment to the section titles in the list of
Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled ``History''
in the various original documents, forming one section Entitled
``History''; likewise combine any sections Entitled ``Acknowledgements'',
and any sections Entitled ``Dedications''. You must delete all
sections Entitled ``Endorsements.''

@item
COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents
released under this License, and replace the individual copies of this
License in the various documents with a single copy that is included in
the collection, provided that you follow the rules of this License for
verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute
it individually under this License, provided you insert a copy of this
License
into the extracted document, and follow this License in all
other respects regarding verbatim copying of that document.

@item
AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate
and independent documents or works, in or on a volume of a storage or
distribution medium, is called an ``aggregate'' if the copyright
resulting from the compilation is not used to limit the legal rights
of the compilation's users beyond what the individual works permit.
When the Document is included in an aggregate, this License does not
apply to the other works in the aggregate which are not themselves
derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these
copies of the Document, then if the Document is less than one half of
the entire aggregate, the Document's Cover Texts may be placed on
covers that bracket the Document within the aggregate, or the
electronic equivalent of covers if the Document is in electronic
form.
Otherwise they must appear on printed covers that bracket the whole
aggregate.

@item
TRANSLATION

Translation is considered a kind of modification, so you may
distribute translations of the Document under the terms of section 4.
Replacing Invariant Sections with translations requires special
permission from their copyright holders, but you may include
translations of some or all Invariant Sections in addition to the
original versions of these Invariant Sections. You may include a
translation of this License, and all the license notices in the
Document, and any Warranty Disclaimers, provided that you also include
the original English version of this License and the original versions
of those notices and disclaimers. In case of a disagreement between
the translation and the original version of this License or a notice
or disclaimer, the original version will prevail.

If a section in the Document is Entitled ``Acknowledgements'',
``Dedications'', or ``History'', the requirement
(section 4) to Preserve
its Title (section 1) will typically require changing the actual
title.

@item
TERMINATION

You may not copy, modify, sublicense, or distribute the Document
except as expressly provided under this License. Any attempt
otherwise to copy, modify, sublicense, or distribute it is void, and
will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license
from a particular copyright holder is reinstated (a) provisionally,
unless and until the copyright holder explicitly and finally
terminates your license, and (b) permanently, if the copyright holder
fails to notify you of the violation by some reasonable means prior to
60 days after the cessation.

Moreover, your license from a particular copyright holder is
reinstated permanently if the copyright holder notifies you of the
violation by some reasonable means, this is the first time you have
received notice of violation of this License (for any
 work) from that
copyright holder, and you cure the violation prior to 30 days after
your receipt of the notice.

Termination of your rights under this section does not terminate the
licenses of parties who have received copies or rights from you under
this License. If your rights have been terminated and not permanently
reinstated, receipt of a copy of some or all of the same material does
not give you any rights to use it.

@item
FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions
of the GNU Free Documentation License from time to time. Such new
versions will be similar in spirit to the present version, but may
differ in detail to address new problems or concerns. See
@uref{http://www.gnu.org/copyleft/}.

Each version of the License is given a distinguishing version number.
If the Document specifies that a particular numbered version of this
License ``or any later version'' applies to it, you have the option of
following the terms and
 conditions either of that specified version or
of any later version that has been published (not as a draft) by the
Free Software Foundation. If the Document does not specify a version
number of this License, you may choose any version ever published (not
as a draft) by the Free Software Foundation. If the Document

specifies that a proxy can decide which future versions of this
License can be used, that proxy's public statement of acceptance of a
version permanently authorizes you to choose that version for the
Document.

@item
RELICENSING

``Massive Multiauthor Collaboration Site'' (or ``MMC Site'') means any
World Wide Web server that publishes copyrightable works and also
provides prominent facilities for anybody to edit those works. A
public wiki that anybody can edit is an example of such a server. A
``Massive Multiauthor Collaboration'' (or ``MMC'') contained in the
site means any set of copyrightable works thus published on the MMC
site.

``CC-BY-SA'' means the Creative Commons
 Attribution-Share Alike 3.0
license published by Creative Commons Corporation, a not-for-profit
corporation with a principal place of business in San Francisco,
California, as well as future copyleft versions of that license
published by that same organization.

``Incorporate'' means to publish or republish a Document, in whole or
in part, as part of another Document.

An MMC is ``eligible for relicensing'' if it is licensed under this
License, and if all works that were first published under this License
somewhere other than this MMC, and subsequently incorporated in whole
or in part into the MMC, (1) had no cover texts or invariant sections,
and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site
under CC-BY-SA on the same site at any time before August 1, 2009,
provided the MMC is eligible for relicensing.

@end enumerate

@page
@heading ADDENDUM: How to use this License for your documents

To use this License
 in a document you have written, include a copy of
the License in the document and put the following copyright and
license notices just after the title page:

@smallexample
@group

Copyright (C) @var{year} @var{your name}.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.3
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover
Texts. A copy of the license is included in the section entitled ``GNU
Free Documentation License".
@end group
@end smallexample

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts,
replace the ``with@dots{}Texts."@: line with this:

@smallexample
@group
  with the Invariant Sections being @var{list their titles}, with
  the Front-Cover Texts being @var{list}, and with the Back-Cover Texts
  being @var{list}.
@end group
@end smallexample

If you have Invariant
 Sections without Cover Texts, or some other
combination of the three, merge those two alternatives to suit the
situation.

If your document contains nontrivial examples of program code, we
recommend releasing these examples in parallel under your choice of
free software license, such as the GNU General Public License,
to permit their use in free software.

@c Local Variables:
@c ispell-local-pdict: "ispell-dict"
@c End:

1.43 grub 2.02

1.43.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we

have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand
ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees"
and
"recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is

not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered
by this License only if the output, given its
content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed;
section 10
makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of

technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately
publish on each copy an appropriate copyright notice;
keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to
"keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution

medium, is called an
"aggregate" if the compilation and its resulting copyright are not
used to limit the access or legal rights of the compilation's users
beyond what the individual works permit. Inclusion of a covered work
in an aggregate does not cause this License to apply to the other
parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms
of sections 4 and 5, provided that you also convey the
machine-readable Corresponding Source under the terms of this License,
in one of these ways:

a) Convey the object code in, or embodied in, a physical product
(including a physical distribution medium), accompanied by the
Corresponding Source fixed on a durable physical medium
customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product
(including a physical distribution medium), accompanied by a
written offer, valid for at least three years
and valid for as
long as you offer spare parts or customer support for that product
model, to give anyone who possesses the object code either (1) a
copy of the Corresponding Source for all the software in the
product that is covered by this License, on a durable physical
medium customarily used for software interchange, for a price no
more than your reasonable cost of physically performing this
conveying of source, or (2) access to copy the
Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the
written offer to provide the Corresponding Source. This
alternative is allowed only occasionally and noncommercially, and
only if you received the object code with such an offer, in accord
with subsection 6b.

d) Convey the object code by offering access from a designated
place (gratis or for a charge), and offer equivalent access to the
Corresponding Source in
the same way through the same place at no
further charge. You need not require recipients to copy the
Corresponding Source along with the object code. If the place to
copy the object code is a network server, the Corresponding Source
may be on a different server (operated by you or a third party)
that supports equivalent copying facilities, provided you maintain
clear directions next to the object code saying where to find the

Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on

those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above
requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright
holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights
granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of

rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this

License will continue to apply to the part which is the covered work,
but the special requirements of the GNU Affero General Public License,
section 13, concerning interaction through a network will apply to the
combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of
the GNU General Public License from time to time. Such new versions will
be similar in spirit to the present version, but may differ in detail to
address new problems or concerns.

Each version is given a distinguishing version number. If the
Program specifies that a certain numbered version of the GNU General
Public License "or any later version" applies to it, you
have the
option of following the terms and conditions either of that numbered
version or of any later version published by the Free Software
Foundation. If the Program does not specify a version number of the
GNU General Public License, you may choose any version ever published
by the Free Software Foundation.

If the Program specifies that a proxy can decide which future
versions of the GNU General Public License can be used, that proxy's
public statement of acceptance of a version permanently authorizes you
to choose that version for the Program.

Later license versions may give you additional or different
permissions. However, no additional obligations are imposed on any
author or copyright holder as a result of your choosing to follow a
later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY
APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT
HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS"
WITHOUT WARRANTY
OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM
IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF
ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING
WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS

THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17.
Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>
This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what you want to
do, use the GNU Lesser General
Public License instead of this License. But first, please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.
COPYRIGHT AND PERMISSION NOTICE

Copyright 1991-2011 Unicode, Inc. All rights reserved. Distributed under the Terms of Use in
http://www.unicode.org/copyright.html.

Permission is hereby granted, free of charge, to any person obtaining a copy of the Unicode data files and any associated documentation (the "Data Files") or Unicode software and any associated documentation (the "Software") to deal in the Data Files or Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Data Files or Software, and to permit persons to whom the Data Files or Software are furnished to do so, provided that (a) the above copyright notice(s) and this permission notice appear with all copies of the Data Files or Software, (b) both the above copyright notice(s) and this permission notice appear in associated documentation, and (c) there is clear notice in each modified Data File or in the Software as well as in the documentation
associated with the Data File(s) or Software that the data or software has been modified.

THE DATA FILES AND SOFTWARE ARE PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER

IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THE DATA FILES OR SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in these Data Files or Software without prior written authorization of the copyright holder.

1.44 iconv 2.24

1.44.1 Available under license :

GNU LIBRARY GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the library GPL. It is
numbered 2 because it goes with version 2 of the ordinary GPL.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some specially designated Free Software Foundation software, and to any other libraries whose authors decide to use it. You can use it for your libraries, too.

When we speak of free software, we are referring to freedom, not
price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library, or if you modify it.

For example, if you distribute copies of the library, whether gratis

or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link a program with the library, you must provide complete object files to the recipients so that they can relink them with the library, after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

Our method of protecting your rights has two steps: (1) copyright the library, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the library.

Also, for each distributor's protection, we want to make certain that everyone understands that there is no warranty for this free library. If the library is modified by someone else and passed on, we want its recipients to know that what they have is not the original version, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that companies distributing free software will individually obtain patent licenses, thus in effect transforming the program into proprietary software. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License, which was designed for utility programs. This license, the GNU Library General Public License, applies to certain designated libraries. This license is quite different from the ordinary one; be sure to read it in full, and don't assume that anything in it is the same as in the ordinary license.

The reason we have a separate public license for some libraries is that they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and legal sense, the linked executable is a combined work, a derivative of the original library, and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public License for libraries did not effectively promote software sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

GNU LIBRARY GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent
of the use of the Library in a tool for
writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must
itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this

function must
be optional: if the application does not supply it, the square
root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition,
mere aggregation of another work not based on the Library
with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of
the
Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a

medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also compile or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

c) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

d) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not

excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute
the Library at all. For example, if a patent
license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system;
it is up to the author/donor to decide if he or she is willing
to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Library General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each
version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a

license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Appendix: How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is

safest to attach them to the start of each source file to most effectively
convey the exclusion of warranty; and each file should have at least the
"copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year>
<name of author>

This library is free software; you can redistribute it and/or
modify it under the terms of the GNU Library General Public
License as published by the Free Software Foundation; either
version 2 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
Library General Public License for more details.

You should have received a copy of the GNU Library General Public
License along with this library; if not, write to the Free
Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston,
MA 02110-1301, USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the library, if
necessary.
Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the
library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!
GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for
software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we

stand
ready to extend this provision to those domains in future versions
of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents.
States should not allow patents to restrict development and use of
software on general-purpose computers, but in those that do, we wish to
avoid the special danger that patents applied to a free program could
make it effectively proprietary. To prevent this, the GPL assures that
patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and
modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of
works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this
License. Each licensee is addressed as "you". "Licensees"
and
"recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work
in a fashion requiring copyright permission, other than the making of an
exact copy. The resulting work is called a "modified version" of the
earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based
on the Program.

To "propagate" a work means to do anything with it that, without
permission, would make you directly or secondarily liable for
infringement under applicable copyright law, except executing it on a
computer or modifying a private copy. Propagation includes copying,
distribution (with or without modification), making available to the
public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other
parties to make or receive copies. Mere interaction with a user through
a computer network, with no transfer of a copy, is
not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The
"System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally
available free
programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding

Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered
by this License only if the output, given its
content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed;
section 10
makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately
publish on each copy an appropriate copyright notice;
keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to
"keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution
medium, is called an
"aggregate" if the compilation and its resulting copyright are not

used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is

available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates

for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or

authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on

those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above
requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is

reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright
holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights
granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that

any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or

arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License,

section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE

USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17.
Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>
This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what you want to
do, use the GNU Lesser General
Public License instead of this License. But first, please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.

1.45 libgcrypt 1.7.3

1.45.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it. (Some other Free Software Foundation software is covered by
the GNU Library General Public License instead.) You can apply it to

your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed

under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this

License. (Exception: if the Program itself is interactive but
does not normally print such an announcement, your work based on
the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If
identifiable sections of that work are not derived from the Program,
and can be reasonably considered
independent and separate works in
themselves, then this License, and its terms, do not apply to those
sections when you distribute them as separate works. But when you
distribute the same sections as part of a whole which is a work based
on the Program, the distribution of the whole must be on the terms of
this License, whose permissions for other licensees extend to the
entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest
your rights to work written entirely by you; rather, the intent is to
exercise the right to control the distribution of derivative or
collective works based on the Program.

In addition, mere aggregation of another work not based on the Program
with the Program (or with a work based on the Program) on a volume of
a storage or distribution medium does not bring the other work under
the scope of this License.

3. You may copy and distribute the Program (or a work based
on it,
under Section 2) in object code or executable form under the terms of
Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable
source code, which must be distributed under the terms of Sections
1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three
years, to give any third party, for a charge no more than your
cost of physically performing source distribution, a complete
machine-readable copy of the corresponding source code, to be
distributed under the terms of Sections 1 and 2 above on a medium
customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer
to distribute corresponding source code. (This alternative is
allowed only for noncommercial distribution and only if you
received the program in object code or
executable form with such
an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the
source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each
time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not

excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free

Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW.
EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN
IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation; either version 2 of the License,
or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and
`show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may

consider it more useful to permit linking proprietary applications with the
library. If this is what you want to do, use the GNU Library General
Public License instead of this License.
Additional license notices for Libgcrypt. -*- org -*-

This file contains the copying permission notices for various files in
the Libgcrypt distribution which are not covered by the GNU Lesser
General Public License (LGPL) or the GNU General Public License (GPL).

These notices all require that a copy of the notice be included
in the accompanying documentation and be distributed with binary
distributions of the code, so be sure to include this file along
with any binary distributions derived from the GNU C Library.

* BSD_3Clause

 For files:
 - cipher/sha256-avx-amd64.S
 - cipher/sha256-avx2-bmi2-amd64.S
 - cipher/sha256-ssse3-amd64.S
 - cipher/sha512-avx-amd64.S
 - cipher/sha512-avx2-bmi2-amd64.S
 - cipher/sha512-ssse3-amd64.S

#+begin_quote
 Copyright (c) 2012, Intel Corporation

 All rights reserved.

 Redistribution and use in source and binary forms, with or without
 modification, are permitted provided that the following conditions are
 met:

 * Redistributions
 of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.

 * Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the
   distribution.

 * Neither the name of the Intel Corporation nor the names of its
   contributors may be used to endorse or promote products derived from
   this software without specific prior written permission.

 THIS SOFTWARE IS PROVIDED BY INTEL CORPORATION "AS IS" AND ANY

EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL INTEL CORPORATION OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
LOSS OF USE, DATA, OR
PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
#+end_quote

For files:
- random/jitterentropy-base.c
- random/jitterentropy.h
- random/rndjent.c (plus common Libgcrypt copyright holders)

#+begin_quote
* Copyright Stephan Mueller <smueller@chronox.de>, 2013
*
* License
* =======
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the above copyright
*   notice, and the entire permission notice in its entirety,
*   including the disclaimer of warranties.
* 2. Redistributions in binary form must reproduce the above copyright
*   notice, this list of conditions and the
following disclaimer in the
*   documentation and/or other materials provided with the distribution.
* 3. The name of the author may not be used to endorse or promote
*   products derived from this software without specific prior
*   written permission.
*
* ALTERNATIVELY, this product may be distributed under the terms of
* the GNU General Public License, in which case the provisions of the GPL are
* required INSTEAD OF the above restrictions. (This clause is
* necessary due to a potential bad interaction between the GPL and
* the restrictions contained in a BSD-style copyright.)
*
* THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED
* WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
* OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ALL OF

* WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE
* LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
* CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
 PROCUREMENT
* OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
* BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
* LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
* (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
* USE OF THIS SOFTWARE, EVEN IF NOT ADVISED OF THE POSSIBILITY OF SUCH
* DAMAGE.
#+end_quote

* X License

 For files:
 - install.sh

#+begin_quote
 Copyright (C) 1994 X Consortium

 Permission is hereby granted, free of charge, to any person obtaining a copy
 of this software and associated documentation files (the "Software"), to
 deal in the Software without restriction, including without limitation the
 rights to use, copy, modify, merge, publish, distribute, sublicense, and/or
 sell copies of the Software, and to permit persons to whom the Software is
 furnished to do so, subject to the following conditions:

 The above copyright notice and this permission notice shall be included in
 all copies or
 substantial portions of the Software.

 THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
 IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
 FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
 X CONSORTIUM BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN
 AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNEC-
 TION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

 Except as contained in this notice, the name of the X Consortium shall not
 be used in advertising or otherwise to promote the sale, use or other deal-
 ings in this Software without prior written authorization from the X Consor-
 tium.
#+end_quote

* Public domain

 For files:
 - cipher/arcfour-amd64.S

#+begin_quote
Author: Marc Bevand <bevand_m (at) epita.fr>
Licence: I hereby disclaim the copyright on this code and place it
in the public domain.
#+end_quote

* OCB license 1

For
files:
- cipher/cipher-ocb.c

#+begin_quote
OCB is covered by several patents but may be used freely by most
software. See http://web.cs.ucdavis.edu/~rogaway/ocb/license.htm .
In particular license 1 is suitable for Libgcrypt: See
http://web.cs.ucdavis.edu/~rogaway/ocb/license1.pdf for the full
license document; it basically says:

License 1 License for Open-Source Software Implementations of OCB
(Jan 9, 2013)

Under this license, you are authorized to make, use, and
distribute open-source software implementations of OCB. This
license terminates for you if you sue someone over their
open-source software implementation of OCB claiming that you have
a patent covering their implementation.

License for Open Source Software Implementations of OCB
January 9, 2013

1 Definitions

1.1 Licensor means Phillip Rogaway.

1.2 Licensed Patents means any patent that claims priority to United
States Patent Application No. 09/918,615 entitled
Method and Apparatus
for Facilitating Efficient Authenticated Encryption, and any utility,
divisional, provisional, continuation, continuations-in-part, reexamination,
reissue, or foreign counterpart patents that may issue with respect to the
aforesaid patent application. This includes, but is not limited to, United
States Patent No. 7,046,802; United States Patent No. 7,200,227; United
States Patent No. 7,949,129; United States Patent No. 8,321,675 ; and any
patent that issues out of United States Patent Application No. 13/669,114.

1.3 Use means any practice of any invention claimed in the Licensed Patents.

1.4 Software Implementation means any practice of any invention claimed in the Licensed Patents that takes the form of software executing on a user-programmable, general-purpose computer or that takes the form of a computer-readable medium storing such software. Software Implementation does not include, for example, application-specific integrated circuits (ASICs), field-programmable gate arrays (FPGAs), embedded systems, or IP cores.

1.5 Open Source Software means software whose source code is published and made available for inspection and use by anyone because either (a) the source code is subject to a license that permits recipients to copy, modify, and distribute the source code without payment of fees or royalties, or (b) the source code is in the public domain, including code released for public use through a CC0 waiver. All licenses certified by the Open Source Initiative at opensource.org as of January 9, 2013 and all Creative Commons licenses identified on the creativecommons.org website as of January 9, 2013, including the Public License Fallback of the CC0 waiver, satisfy these requirements for the purposes of this license.

1.6 Open Source Software Implementation means a Software Implementation in which the software implicating the Licensed Patents is Open Source Software. Open Source Software Implementation does not include
any Software Implementation in which the software implicating the Licensed Patents is combined, so as to form a larger program, with software that is not Open Source Software.

2 License Grant

2.1 License. Subject to your compliance with the term s of this license, including the restriction set forth in Section 2.2, Licensor hereby grants to you a perpetual, worldwide, non-exclusive, non-transferable, non-sublicenseable, no-charge, royalty-free, irrevocable license to practice any invention claimed in the Licensed Patents in any Open Source Software Implementation.

2.2 Restriction. If you or your affiliates institute patent litigation (including, but not limited to, a cross-claim or counterclaim in a lawsuit) against any entity alleging that any Use authorized by this license infringes another patent, then any rights granted to you under this license automatically terminate as of the date such litigation is filed.

3 Disclaimer
YOUR USE OF THE LICENSED PATENTS
IS AT YOUR OWN RISK AND UNLESS REQUIRED
BY APPLICABLE LAW, LICENSOR MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY

KIND CONCERNING THE LICENSED PATENTS OR ANY PRODUCT EMBODYING ANY LICENSED PATENT, EXPRESS OR IMPLIED, STATUT ORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MERCHANTIBILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL LICENSOR BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM OR RELATED TO ANY USE OF THE LICENSED PATENTS, INCLUDING, WITHOUT LIMITATION, DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR SPECIAL DAMAGES, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES PRIOR TO SUCH AN OCCURRENCE.
#+end_quote

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts
as the successor of the GNU Library Public License, version 2, hence
the version number 2.1.]

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
Licenses are intended to guarantee your freedom to share and change
free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some
specially designated software packages--typically libraries--of the
Free Software Foundation and other authors who
decide to use it. You
can use it too, but we suggest you first think carefully about whether
this license or the ordinary General Public License is the better
strategy to use in any particular case, based on the explanations
below.

When we speak of free software, we are referring to freedom of use,
not price. Our General Public Licenses are designed to make sure that
you have the freedom to distribute copies of free software (and charge
for this service if you wish); that you receive source code or can get
it if you want it; that you can change the software and use pieces of
it in new free programs; and that you are informed that you can do
these things.

To protect your rights, we need to make restrictions that forbid

distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library,
whether gratis
or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.
^L
Finally, software
patents pose a constant threat to the existence of
any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits
such linking only if the
entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting
the free library to free
software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order
to run.
^L
GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no

charge to all third parties under
the terms of this License.

d) If a facility in the modified Library refers to a function or a
table of data to be supplied by an application program that uses
the facility, other than as an argument passed when the facility
is invoked, then you must make a good faith effort to ensure that,
in the event an application does not supply such function or
table, the facility still operates, and performs whatever part of
its purpose remains meaningful.

(For example, a function in a library to compute square roots has
a purpose that is entirely well-defined independent of the
application. Therefore, Subsection 2d requires that any
application-supplied function or table used by this function must
be optional: if the application does not supply it, the square
root function must still compute square roots.)

These requirements apply to the modified work as a whole. If
identifiable sections of that work are not derived from the Library,
and can
be reasonably considered independent and separate works in
themselves, then this License, and its terms, do not apply to those
sections when you distribute them as separate works. But when you
distribute the same sections as part of a whole which is a work based
on the Library, the distribution of the whole must be on the terms of
this License, whose permissions for other licensees extend to the
entire whole, and thus to each and every part regardless of who wrote
it.

Thus, it is not the intent of this section to claim rights or contest
your rights to work written entirely by you; rather, the intent is to
exercise the right to control the distribution of derivative or
collective works based on the Library.

In addition, mere aggregation of another work not based on the Library
with the Library (or with a work based on the Library) on a volume of
a storage or distribution medium does not bring the other work under
the scope of this License.

3. You may opt to apply the terms of the
ordinary GNU General Public
License instead of this License to a given copy of the Library. To do
this, you must alter all the notices that refer to this License, so
that they refer to the ordinary GNU General Public License, version 2,
instead of to this License. (If a newer version than version 2 of the
ordinary GNU General Public License has appeared, then you can specify
that version instead if you wish.) Do not make any other change in

these notices.
^L
Once this change is made in a given copy, it is irreversible for
that copy, so the ordinary GNU General Public License applies to all
subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of
the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or
derivative of it, under Section 2) in object code or executable form
under the terms of Sections 1 and 2 above provided that you accompany
it with the complete
corresponding machine-readable source code, which
must be distributed under the terms of Sections 1 and 2 above on a
medium customarily used for software interchange.

If distribution of object code is made by offering access to copy
from a designated place, then offering equivalent access to copy the
source code from the same place satisfies the requirement to
distribute the source code, even though third parties are not
compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the
Library, but is designed to work with the Library by being compiled or
linked with it, is called a "work that uses the Library". Such a
work, in isolation, is not a derivative work of the Library, and
therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library
creates an executable that is a derivative of the Library (because it
contains portions of the Library), rather than a "work
that uses the
library". The executable is therefore covered by this License.
Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file
that is part of the Library, the object code for the work may be a
derivative work of the Library even though the source code is not.
Whether this is true is especially significant if the work can be
linked without the Library, or if the work is itself a library. The
threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data
structure layouts and accessors, and small macros and small inline
functions (ten lines or less in length), then the use of the object
file is unrestricted, regardless of whether it is legally a derivative
work. (Executables containing this object code plus portions of the

Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute
the object code for the work under the terms of Section 6.
Any executables containing that work also fall under Section 6,
whether or not they are linked directly with the Library itself.
^L
6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a)
Accompany the work with the complete corresponding
machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will
operate properly with a modified version of the library, if
the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of

performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.
^L
7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses

terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited
by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.
^L
11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they
do not
excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution
system which is
implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing

to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.
^L
14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME

THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED
ABOVE, BE LIABLE TO YOU
FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

^L

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file
to most
effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston,

MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or
your school, if any, to sign a "copyright disclaimer" for the library,
if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the
library `Frob' (a library for tweaking knobs) written by James
Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

1.46 fuse 2.9.4

1.46.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it. (Some other Free Software Foundation software is covered by
the GNU Lesser General Public License instead.) You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price.
Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which
gives you legal permission to copy,
distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of

running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you

distribute the same sections as part of a whole which is a work based
on the Program, the distribution of the whole must be on the terms of
this License, whose permissions for other licensees extend to the
entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest
your rights to work written entirely by you; rather, the intent is to
exercise the right to control the distribution of derivative or
collective works based on the Program.

In addition, mere aggregation of another work not based on the Program
with the Program (or with a work based on the Program) on a volume of
a storage or distribution medium does not bring the other work under
the scope of this License.

3. You may copy and distribute the Program (or a work based on it,
under Section 2) in object code or executable form under the terms of
Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable
source code, which must be distributed under the terms of Sections
1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three
years, to give any third party, for a charge no more than your
cost of physically performing source distribution, a complete
machine-readable copy of the corresponding source code, to be
distributed under the terms of Sections 1 and 2 above on a medium
customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer
to distribute corresponding source code. (This alternative is
allowed only for noncommercial distribution
and only if you
received the program in object code or executable form with such
an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for
making modifications to it. For an executable work, complete source
code means all the source code for all modules it contains, plus any
associated interface definition files, plus the scripts used to
control compilation and installation of the executable. However, as a
special exception, the source code distributed need not include
anything that is normally distributed (in either source or binary
form) with the major components (compiler, kernel, and so on) of the
operating system on which the executable runs, unless that component
itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under

any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE,
THERE IS NO WARRANTY
FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR
THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU
General Public License as published by
the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful,

but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License along
with this program; if not, write to the Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute
it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this
is what you want to do, use the GNU Lesser General
Public License instead of this License.

1.47 lighttpd 1.4.41

1.47.1 Available under license :

Copyright (c) 2004, Jan Kneschke, incremental

All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this
 list of conditions and the following disclaimer.

- Redistributions in binary form must reproduce the above copyright notice,
 this list of conditions and the following disclaimer in the documentation
 and/or other materials provided with the distribution.

- Neither the name of the 'incremental' nor the names of its contributors may
 be used to endorse or promote products derived from this software without
 specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL
 THE COPYRIGHT OWNER OR CONTRIBUTORS BE
LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF
THE POSSIBILITY OF SUCH DAMAGE.

1.48 gnupg 2.1.14

1.48.1 Available under license :

Here is a list with collected copyright notices. For details see the
description of each individual package. [Compiled by wk 2017-11-07]

GNUPG is

Copyright (C) 1997-2017 Werner Koch
Copyright (C) 1994-2017 Free Software Foundation, Inc.
Copyright (C) 2003-2017 g10 Code GmbH
Copyright (C) 2002 Klarlvdalens Datakonsult AB
Copyright (C) 1995-1997, 2000-2007 Ulrich Drepper <drepper@gnu.ai.mit.edu>
Copyright (C) 1994 X Consortium
Copyright (C) 1998 by The Internet Society.
Copyright (C) 1998-2004 The OpenLDAP Foundation
Copyright (C) 1998-2004 Kurt D. Zeilenga.

Copyright (C) 1998-2004 Net Boolean Incorporated.
Copyright (C) 2001-2004 IBM Corporation.
Copyright (C) 1999-2003 Howard Y.H. Chu.
Copyright (C) 1999-2003 Symas Corporation.
Copyright (C) 1998-2003 Hallvard B. Furuseth.
Copyright (C) 1992-1996 Regents of the University of Michigan.
Copyright (C) 2000 Dimitrios Souflis
Copyright (C) 2008,2009,2010,2012-2016 William Ahern

GnuPG is free software;
you can redistribute it and/or modify it
under the terms of the GNU General Public License as published by
the Free Software Foundation; either version 3 of the License, or
(at your option) any later version.

GnuPG is distributed in the hope that it will be useful, but WITHOUT
ANY WARRANTY; without even the implied warranty of MERCHANTABILITY
or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public
License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, see <https://www.gnu.org/licenses/>.

LIBGCRYPT is

Copyright (C) 1989,1991-2017 Free Software Foundation, Inc.
Copyright (C) 1994 X Consortium
Copyright (C) 1996 L. Peter Deutsch
Copyright (C) 1997 Werner Koch
Copyright (C) 1998 The Internet Society
Copyright (C) 1996-1999 Peter Gutmann, Paul Kendall, and Chris Wedgwood
Copyright (C) 1996-2006 Peter Gutmann, Matt Thomlinson and Blake Coverett
Copyright (C) 2003 Nikos Mavroyanopoulos
Copyright (C) 2006-2007 NTT (Nippon Telegraph and Telephone Corporation)
Copyright (C) 2012-2017 g10 Code GmbH
Copyright (C) 2012 Simon Josefsson, Niels Mller
Copyright (c) 2012 Intel Corporation
Copyright (C) 2013 Christian Grothoff
Copyright (C) 2013-2017 Jussi Kivilinna
Copyright (C) 2013-2014 Dmitry Eremin-Solenikov
Copyright (C) 2014 Stephan Mueller
Copyright (C) 2017 Bundesamt fr Sicherheit in der Informationstechnik

Libgcrypt is free software; you can redistribute it and/or modify
it under the terms of the GNU Lesser General Public License as
published by the Free Software Foundation; either version 2.1 of
the License, or (at your option) any later version.

Libgcrypt is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU Lesser General Public License for more details.

You should have received a copy of the
GNU Lesser General Public
License along with this program; if not, see <http://www.gnu.org/licenses/>.

LIBGPG-ERROR is

Copyright (C) 2003-2004, 2010, 2013-2017 g10 Code GmbH

libgpg-error is free software; you can redistribute it and/or
modify it under the terms of the GNU Lesser General Public License
as published by the Free Software Foundation; either version 2.1 of
the License, or (at your option) any later version.

libgpg-error is distributed in the hope that it will be useful, but
WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License
along with this program; if not, see <http://www.gnu.org/licenses/>.

LIBASSUAN is

Copyright (C) 1992-2013 Free Software Foundation, Inc.
Copyright (C) 1994 X Consortium
Copyright (C) 2000 Werner Koch (dd9jn)
Copyright (C)
2001-2016 g10 Code GmbH
Copyright (C) 2004 Simon Josefsson

Assuan is free software; you can redistribute it and/or modify it
under the terms of the GNU Lesser General Public License as
published by the Free Software Foundation; either version 2.1 of
the License, or (at your option) any later version.

Assuan is distributed in the hope that it will be useful, but
WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public
License along with this program; if not, see <http://www.gnu.org/licenses/>.

LIBKSBA is

Copyright (C) 2001, 2002, 2003, 2004, 2005, 2006, 2010, 2011
2012, 2013, 2014, 2015 g10 Code GmbH
Copyright (C) 2001, 2002, 2003, 2007 Free Software Foundation, Inc.
Copyright (C) 2000, 2001 Fabio Fiorina

The library and the header files are distributed under
the following
terms (LGPLv3+/GPLv2+):

KSBA is free software; you can redistribute it and/or modify
it under the terms of either

- the GNU Lesser General Public License as published by the Free
Software Foundation; either version 3 of the License, or (at
your option) any later version.

or

- the GNU General Public License as published by the Free
Software Foundation; either version 2 of the License, or (at
your option) any later version.

or both in parallel, as here.

KSBA is distributed in the hope that it will be useful, but WITHOUT
ANY WARRANTY; without even the implied warranty of MERCHANTABILITY
or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public
License for more details.

The other parts (e.g. manual, build system, tests) are distributed
under the following terms (GPLv3):

KSBA is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the
Free Software Foundation; either version 3 of the License, or
(at your option) any later version.

KSBA is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

NPTH is

Copyright (C) 2011, 2012, 2014, 2015, 2017 g10 Code GmbH

nPth is free software; you can redistribute it and/or modify
it under the terms of the GNU Lesser General Public License as
published by the Free Software Foundation; either version 2.1 of
the License, or (at your option) any later version.

nPth is distributed in the hope that it will be useful, but
WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See
the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public
License along with this program;
if not, see <https://www.gnu.org/licenses/>.

NTBTLS is

Copyright (C) 2006-2014 Brainspark B.V.
Copyright (C) 2014-2017 g10 Code GmbH

NTBTLS is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation; either version 3 of the License, or
(at your option) any later version.

NTBTLS is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, see <http://www.gnu.org/licenses/>.

PINENTRY is

Copyright (C) 1999 Robert Bihlmeyer <robbe@orcus.priv.at>
Copyright (C) 2001-2004, 2007-2008, 2010, 2015-2016 g10 Code GmbH
Copyright (C) 2002, 2008 Klarlvdalens Datakonsult AB (KDAB)
Copyright (C) 2004 by Albrecht
Dre <albrecht.dress@arcor.de>
Copyright 2007 Ingo Klcker

Copyright (C) 2014 Serge Voilokov
Copyright (C) 2015 Daiki Ueno
Copyright (C) 2015 Daniel Kahn Gillmor <dkg@fifthhorseman.net>
Copyright 2016 Intevation GmbH

PINENTRY is free software; you can redistribute it and/or modify it
under the terms of the GNU General Public License as published by
the Free Software Foundation; either version 2 of the License, or
(at your option) any later version.

PINENTRY is distributed in the hope that it will be useful, but
WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, see <https://www.gnu.org/licenses/>.

GPGME is

Copyright (C) 1991-2013 Free Software Foundation, Inc.
Copyright (C) 2000-2001 Werner Koch
Copyright (C) 2001-2017 g10 Code GmbH

Copyright (C) 2002 Klarlvdalens Datakonsult AB
Copyright (C) 2004-2008 Igor Belyi
Copyright (C) 2002 John Goerzen
Copyright (C) 2014, 2015 Martin Albrecht
Copyright (C) 2015 Ben McGinnes
Copyright (C) 2015-2016 Bundesamt fr Sicherheit in der Informationstechnik
Copyright (C) 2016 Intevation GmbH

GPGME is free software; you can redistribute it and/or modify it
under the terms of the GNU Lesser General Public License as
published by the Free Software Foundation; either version 2.1 of
the License, or (at your option) any later version.

GPGME is distributed in the hope that it will be useful, but
WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License
along with this program; if not, see <http://www.gnu.org/licenses/>.

NSIS is

Copyright 1999-2009 Nullsoft and Contributors
Copyright 2002-2008 Amir Szekely
Copyright 2003 Ramon

This license applies to everything in the NSIS package, except where otherwise noted.

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

The user interface used with the installer is

Copyright 2002-2009 Joost Verburg

[It is distributed along with NSIS and the same conditions as stated above apply]

TinySCHEME is part of the GnuPG package and is

Copyright (c) 2000, Dimitrios Souflis
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright

notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

Neither the name of Dimitrios Souflis nor the names of the
contributors may be used to endorse or promote products derived from
this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED
BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR
PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

LIBDNS is part of the GnuPG package and is

Copyright (c) 2008, 2009, 2010, 2012-2016 William Ahern

Permission is hereby granted, free of charge, to any person obtaining a
copy of this software and associated documentation files (the
"Software"),
to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to permit
persons to whom the Software is furnished to do so, subject to the
following conditions:

The above copyright notice and this permission notice shall be included
in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS
OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN
NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM,
DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR
OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE
USE OR OTHER DEALINGS IN THE SOFTWARE.

ZLIB is

(C) 1995-2013 Jean-loup Gailly and Mark Adler

This software is provided
'as-is', without any express or implied
warranty. In no event will the authors be held liable for any damages
arising from the use of this software.

Permission is granted to anyone to use this software for any purpose,
including commercial applications, and to alter it and redistribute it
freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not
   claim that you wrote the original software. If you use this software
   in a product, an acknowledgment in the product documentation would be
   appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be
   misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly Mark Adler
jloup@gzip.org madler@alumni.caltech.edu

BZIP2 is

This program, "bzip2", the associated library "libbzip2", and all
documentation,
are copyright (C) 1996-2010 Julian R Seward. All
rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.

2. The origin of this software must not be misrepresented; you must
   not claim that you wrote the original software. If you use this
   software in a product, an acknowledgment in the product
   documentation would be appreciated but is not required.

3. Altered source versions must be plainly marked as such, and must
   not be misrepresented as being the original software.

4. The name of the author may not be used to endorse or promote
   products derived from this software without specific prior written
   permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS" AND ANY EXPRESS
OR IMPLIED WARRANTIES,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY
DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE
GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

SQLITE has

been put into the public-domain by its author D. Richard Hipp:
The author disclaims copyright to this source code. In place of
a legal notice, here is a blessing:

May you do good and not evil.
May you find forgiveness for yourself and forgive others.
May you share freely, never taking more than you give.

[Note that only a few files are distributed under this license.]

Creative Commons Legal Code

CC0 1.0 Universal

CREATIVE COMMONS CORPORATION IS NOT A LAW FIRM AND DOES NOT PROVIDE
LEGAL SERVICES. DISTRIBUTION OF THIS DOCUMENT DOES NOT CREATE AN
ATTORNEY-CLIENT RELATIONSHIP. CREATIVE COMMONS PROVIDES THIS
INFORMATION ON AN "AS-IS" BASIS. CREATIVE COMMONS MAKES NO WARRANTIES
REGARDING THE USE OF THIS DOCUMENT OR THE INFORMATION OR WORKS
PROVIDED HEREUNDER, AND DISCLAIMS LIABILITY FOR DAMAGES RESULTING FROM
THE USE OF THIS DOCUMENT OR THE INFORMATION OR WORKS PROVIDED
HEREUNDER.

Statement of Purpose

The laws of most jurisdictions throughout the world automatically confer
exclusive Copyright and Related Rights (defined below) upon the creator
and subsequent owner(s) (each and all, an "owner") of an original work of
authorship and/or a database (each, a "Work").

Certain owners wish to permanently relinquish those rights to a Work for
the purpose of contributing

to a commons of creative, cultural and
scientific works ("Commons") that the public can reliably and without fear of later claims of infringement build upon, modify, incorporate in other works, reuse and redistribute as freely as possible in any form whatsoever and for any purposes, including without limitation commercial purposes. These owners may contribute to the Commons to promote the ideal of a free culture and the further production of creative, cultural and scientific works, or to gain reputation or greater distribution for their Work in part through the use and efforts of others.

For these and/or other purposes and motivations, and without any expectation of additional consideration or compensation, the person associating CC0 with a Work (the "Affirmer"), to the extent that he or she is an owner of Copyright and Related Rights in the Work, voluntarily elects to apply CC0 to the Work and publicly distribute the Work under its terms, with knowledge of his or her Copyright
and Related Rights in the
Work and the meaning and intended legal effect of CC0 on those rights.

1. Copyright and Related Rights. A Work made available under CC0 may be protected by copyright and related or neighboring rights ("Copyright and Related Rights"). Copyright and Related Rights include, but are not limited to, the following:

i. the right to reproduce, adapt, distribute, perform, display, communicate, and translate a Work;
ii. moral rights retained by the original author(s) and/or performer(s);
iii. publicity and privacy rights pertaining to a person's image or likeness depicted in a Work;
iv. rights protecting against unfair competition in regards to a Work, subject to the limitations in paragraph 4(a), below;
v. rights protecting the extraction, dissemination, use and reuse of data in a Work;
vi. database rights (such as those arising under Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection
of databases, and under any national implementation thereof, including any amended or successor version of such directive); and
vii. other similar, equivalent or corresponding rights throughout the world based on applicable law or treaty, and any national implementations thereof.

2. Waiver. To the greatest extent permitted by, but not in contravention of, applicable law, Affirmer hereby overtly, fully, permanently, irrevocably and unconditionally waives, abandons, and surrenders all of Affirmer's Copyright and Related Rights and associated claims and causes of action, whether now known or unknown (including existing as well as

future claims and causes of action), in the Work (i) in all territories worldwide, (ii) for the maximum duration provided by applicable law or treaty (including future time extensions), (iii) in any current or future medium and for any number of copies, and (iv) for any purpose whatsoever, including without limitation commercial, advertising or promotional purposes (the "Waiver"). Affirmer makes the Waiver for the benefit of each member of the public at large and to the detriment of Affirmer's heirs and successors, fully intending that such Waiver shall not be subject to revocation, rescission, cancellation, termination, or any other legal or equitable action to disrupt the quiet enjoyment of the Work by the public as contemplated by Affirmer's express Statement of Purpose.

3. Public License Fallback. Should any part of the Waiver for any reason be judged legally invalid or ineffective under applicable law, then the Waiver shall be preserved to the maximum extent permitted taking into account Affirmer's express Statement of Purpose. In addition, to the extent the Waiver is so judged Affirmer hereby grants to each affected person a royalty-free, non transferable, non sublicensable, non exclusive, irrevocable and unconditional license to exercise Affirmer's Copyright and Related Rights in the Work (i) in all territories worldwide, (ii) for the maximum duration provided by applicable law or treaty (including future time extensions), (iii) in any current or future medium and for any number of copies, and (iv) for any purpose whatsoever, including without limitation commercial, advertising or promotional purposes (the "License"). The License shall be deemed effective as of the date CC0 was applied by Affirmer to the Work. Should any part of the License for any reason be judged legally invalid or ineffective under applicable law, such partial invalidity or ineffectiveness shall not invalidate the remainder of the License, and in such case Affirmer hereby affirms that he or she will not (i) exercise any of his or her remaining Copyright and Related Rights in the Work or (ii) assert any associated claims and causes of action with respect to the Work, in either case contrary to Affirmer's express Statement of Purpose.

4. Limitations and Disclaimers.

a. No trademark or patent rights held by Affirmer are waived, abandoned, surrendered, licensed or otherwise affected by this document.
b. Affirmer offers the Work as-is and makes no representations or warranties of any kind concerning the Work, express, implied, statutory or otherwise, including without limitation warranties of title, merchantability, fitness for a particular purpose, non infringement, or the absence of latent or other defects, accuracy, or the present or absence of errors, whether or not discoverable, all to the greatest extent permissible under applicable law.

c. Affirmer disclaims responsibility for clearing rights of other persons
that may apply to the Work or any use thereof, including without
limitation any person's Copyright and Related Rights in the Work.
Further, Affirmer disclaims responsibility for obtaining any necessary
consents, permissions or other rights required for any use of the
Work.
d. Affirmer understands and acknowledges that Creative Commons is
not a
party to this document and has no duty or obligation with respect to
this CC0 or use of the Work.

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <https://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for
software and other kinds of works.

The licenses for most software and other practical works are designed
to take away your freedom to share and change the works. By contrast,
the GNU General Public License is intended to guarantee your freedom to
share and change all versions of a program--to make sure it remains free
software for all its users. We, the Free Software Foundation, use the
GNU General Public License for most of our software; it applies also to
any other work released this way by its authors. You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price. Our General Public Licenses
are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
them if you wish), that you receive source code or can get it if you
want it, that you can change the software or use pieces of it in new
free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you
these rights or asking you to surrender the rights. Therefore, you have
certain responsibilities if you distribute copies of the software, or if
you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether
gratis or for a fee, you must pass on to the recipients the same
freedoms that you received. You must make sure that they, too, receive

or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To
"modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate
Legal Notices"
to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than
the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an

implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users'
Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep
intact all notices stating that this License and any
non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to

"keep intact all notices".

c) You must license
the entire work, as a whole, under this
License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and
its resulting copyright are not
used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer
support for that product
model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no

more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge.
You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods,

procedures, authorization keys, or other information required to install and execute
modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information
does not include a
requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included
in this License, to the extent
that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of

it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections
15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional
terms are considered "further
restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time
you convey a covered work, the recipient automatically
receives a license from the original licensors, to run, modify and
propagate that work, subject to this License. You are not responsible
for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an
organization, or substantially all assets of one, or subdividing an
organization, or merging organizations. If propagation of a covered
work results from an entity transaction, each party to that
transaction who receives a copy of the work also receives whatever
licenses to the work the party's predecessor in interest had or could
give under the previous paragraph, plus a right to possession of the
Corresponding Source of the work from the predecessor in interest, if
the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the
rights granted or affirmed under this License. For example, you may
not
impose a license fee, royalty, or other charge for exercise of
rights granted under this License, and you may not initiate litigation
(including a cross-claim or counterclaim in a lawsuit) alleging that
any patent claim is infringed by making, using, selling, offering for
sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this
License of the Program or a work on which the Program is based. The
work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims
owned or controlled by the contributor, whether already acquired or
hereafter acquired, that would be infringed by some manner, permitted
by this License, of making, using, or selling its contributor version,
but do not include claims that would be infringed only as a
consequence of further modification of the contributor version. For
purposes of this definition, "control"
includes the right to grant
patent sublicenses in a manner consistent with the requirements of
this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free
patent license under the contributor's essential patent claims, to
make, use, sell, offer for sale, import and otherwise run, modify and
propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express

agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may

otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING,
BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer
of warranty and limitation of liability provided
above cannot be given local legal effect according to their terms,
reviewing courts shall apply local law that most closely approximates
an absolute waiver of all civil liability in connection with the
Program, unless a warranty or assumption of liability accompanies a
copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest

to attach them to the start of each source file to most effectively
state the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where the full notice is found.

  <one line to give the program's name and a brief idea
 of what it does.>
  Copyright (C) <year> <name of author>

  This program is free software: you can redistribute it and/or modify
  it under the terms of the GNU General Public License as published by
  the Free Software Foundation, either version 3 of the License, or
  (at your option) any later version.

  This program is distributed in the hope that it will be useful,
  but WITHOUT ANY WARRANTY; without even the implied warranty of
  MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
  GNU General Public License for more details.

  You should have received a copy of the GNU General Public License
  along with this program. If not, see <https://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

 If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

  <program> Copyright (C) <year> <name of author>
  This program comes with ABSOLUTELY
 NO WARRANTY; for details type `show w'.
  This is free software, and you are welcome to redistribute it
  under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

 You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<https://www.gnu.org/licenses/>.

 The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what you want to do, use the GNU Lesser General
Public License instead of this License. But first,
 please read
<https://www.gnu.org/philosophy/why-not-lgpl.html>.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price.
Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which
gives you legal permission to copy,
distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so

that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices
stating that you changed the files and the date of any change.

b) You must cause
any work that you distribute or publish, that in
whole or in part contains or is derived from the Program or any
part thereof, to be licensed as a whole at no charge to all third
parties under the terms of this License.

c) If the modified program normally reads commands interactively
when run, you must cause it, when started running for such
interactive use in the most ordinary way, to print or display an
announcement including an appropriate copyright notice and a
notice that there is no warranty (or else, saying that you provide
a warranty) and that users may redistribute the program under
these conditions, and telling the user how to view a copy of this
License. (Exception: if the Program itself is interactive but
does not normally print such an announcement, your work based on
the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If
identifiable sections of that work
are not derived from the Program,
and can be reasonably considered independent and separate works in
themselves, then this License, and its terms, do not apply to those
sections when you distribute them as separate works. But when you
distribute the same sections as part of a whole which is a work based
on the Program, the distribution of the whole must be on the terms of
this License, whose permissions for other licensees extend to the
entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest
your rights to work written entirely by you; rather, the intent is to
exercise the right to control the distribution of derivative or
collective works based on the Program.

In addition, mere aggregation of another work not based on the Program
with the Program (or with a work based on the Program) on a volume of
a storage or distribution medium does not bring the other work under
the scope of this License.

3. You may copy and distribute the Program (or a work based on it,
under Section 2) in object code or executable form under the terms of
Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable
source code, which must be distributed under the terms of Sections

1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three
years, to give any third party, for a charge no more than your
cost of physically performing source distribution, a complete
machine-readable copy of the corresponding source code, to be
distributed under the terms of Sections 1 and 2 above on a medium
customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer
to distribute corresponding source code. (This alternative is
allowed only for noncommercial distribution
and only if you
received the program in object code or executable form with such
an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for
making modifications to it. For an executable work, complete source
code means all the source code for all modules it contains, plus any
associated interface definition files, plus the scripts used to
control compilation and installation of the executable. However, as a
special exception, the source code distributed need not include
anything that is normally distributed (in either source or binary
form) with the major components (compiler, kernel, and so on) of the
operating system on which the executable runs, unless that component
itself accompanies the executable.

If distribution of executable or object code is made by offering
access to copy from a designated place, then offering equivalent
access to copy the source code from the same place counts as
distribution of the source
code, even though third parties are not
compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program
except as expressly provided under this License. Any attempt
otherwise to copy, modify, sublicense or distribute the Program is
void, and will automatically terminate your rights under this License.
However, parties who have received copies, or rights, from you under
this License will not have their licenses terminated so long as such
parties remain in full compliance.

5. You are not required to accept this License, since you have not
signed it. However, nothing else grants you permission to modify or
distribute the Program or its derivative works. These actions are
prohibited by law if you do not accept this License. Therefore, by
modifying or distributing the Program (or any work based on the
Program), you indicate your acceptance of this License to do so, and

all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the

original copyright holder who places the Program under this License
may add an explicit geographical distribution limitation excluding
those countries, so that distribution is permitted only in or among
countries not thus excluded. In such case, this License incorporates
the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions
of the General Public License from time to time. Such new versions will
be similar in spirit to the present version, but may differ in detail to
address new problems or concerns.

Each version is given a distinguishing
version number. If the Program
specifies a version number of this License which applies to it and "any
later version", you have the option of following the terms and conditions
either of that version or of any later version published by the Free
Software Foundation. If the Program does not specify a version number of
this License, you may choose any version ever published by the Free Software
Foundation.

10. If you wish to incorporate parts of the Program into other free
programs whose distribution conditions are different, write to the author
to ask for permission. For software which is copyrighted by the Free
Software Foundation, write to the Free Software Foundation; we sometimes
make exceptions for this. Our decision will be guided by the two goals
of preserving the free status of all derivatives of our free software and
of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE,
THERE IS NO WARRANTY
FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES
PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED
OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS
TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE
PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING,
REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING
WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR
REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES,
INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING
OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED
TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY
YOU OR

THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU
General Public License as published by
the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute
it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may

be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

 Yoyodyne, Inc., hereby disclaims all copyright interest in the program
 `Gnomovision' (which makes passes at compilers) written by James Hacker.

 <signature of Ty Coon>, 1 April 1989
 Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this
 is what you want to do, use the GNU Lesser General
Public License instead of this License.
[Note that only a few files are distributed under this license.]

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts
as the successor of the GNU Library Public License, version 2, hence
the version number 2.1.]

Preamble

 The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
Licenses are intended to guarantee your freedom to share and change
free software--to make sure the software is free for all its users.

 This license, the Lesser General Public License, applies to some
specially designated software packages--typically
 libraries--of the
Free Software Foundation and other authors who decide to use it. You
can use it too, but we suggest you first think carefully about whether
this license or the ordinary General Public License is the better
strategy to use in any particular case, based on the explanations
below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected
by problems that might be
introduced by others.
^L
Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.
^L

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim
or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies
of the Library's
complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion

of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under

the
scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public
License instead of this License to a given copy of the Library. To do
this, you must alter all the notices that refer to this License, so
that they refer to the ordinary GNU General Public License, version 2,
instead of to this License. (If a newer version than version 2 of the
ordinary GNU General Public License has appeared, then you can specify
that version instead if you wish.) Do not make any other change in
these notices.
^L
Once this change is made in a given copy, it is irreversible for
that copy, so the ordinary GNU General Public License applies to all
subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of
the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or
derivative of it, under Section 2) in object code or executable form
under the terms of Sections
1 and 2 above provided that you accompany
it with the complete corresponding machine-readable source code, which
must be distributed under the terms of Sections 1 and 2 above on a
medium customarily used for software interchange.

If distribution of object code is made by offering access to copy
from a designated place, then offering equivalent access to copy the
source code from the same place satisfies the requirement to
distribute the source code, even though third parties are not
compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the
Library, but is designed to work with the Library by being compiled or
linked with it, is called a "work that uses the Library". Such a
work, in isolation, is not a derivative work of the Library, and
therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library
creates an executable that is a derivative of the Library
(because it
contains portions of the Library), rather than a "work that uses the
library". The executable is therefore covered by this License.
Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file
that is part of the Library, the object code for the work may be a

derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise,
if the work is a derivative of the Library, you may
distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.
^L
6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy
of this License. Also, you must do one
of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a

copy of the library already present on the user's computer system, rather than
copying library functions into the executable, and (2)
will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the
materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.
^L
7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library
with a copy of the same work
based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact
that part of it is a work based on the Library, and explaining
where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the
Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.
^L
11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement
or
otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole
purpose of protecting the
integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written
in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.
^L
14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the
Free
Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY
OTHER PARTY WHO MAY MODIFY
AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

^L

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It
is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either

version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public
License along with this library; if not, write to the Free
Software
Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or
your school, if any, to sign a "copyright disclaimer" for the library,
if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the
library `Frob' (a library for tweaking knobs) written by James
Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

LICENSE TERMS

Copyright (c) 2000, Dimitrios Souflis
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are
met:

Redistributions of source code must retain the above copyright notice,
this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

Neither the name of Dimitrios Souflis nor the names of the
contributors may be used to endorse or promote products derived from
this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT

LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
IN NO EVENT SHALL THE REGENTS OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
[Note that only a few files are distributed under this license.]

GNU LESSER GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <https://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and the "GNU GPL" refers to version 3 of the GNU General Public License.

"The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An "Application" is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library.
Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without
being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material
is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that,

taken together, effectively do not restrict modification of the
portions of the Library contained in the Combined Work and reverse
engineering for debugging such modifications, if you also do each of
the following:

a) Give prominent notice with each copy of the Combined Work that
the Library is used in it and that the Library and its use are
covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this
license
document.

c) For a Combined Work that displays copyright notices during
execution, include the copyright notice for the Library among
these notices, as well as a reference directing the user to the
copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this
License, and the Corresponding Application Code in a form
suitable for, and under terms that permit, the user to
recombine or relink the Application with a modified version of
the Linked Version to produce a modified Combined Work, in the
manner specified by section 6 of the GNU GPL for conveying
Corresponding Source.

1) Use a suitable shared library mechanism for linking with the
Library. A suitable mechanism is one that (a) uses at run time
a copy of the Library already present on the user's computer
system, and (b) will operate properly with
a modified version
of the Library that is interface-compatible with the Linked
Version.

e) Provide Installation Information, but only if you would otherwise
be required to provide such information under section 6 of the
GNU GPL, and only to the extent that such information is
necessary to install and execute a modified version of the
Combined Work produced by recombining or relinking the
Application with a modified version of the Linked Version. (If
you use option 4d0, the Installation Information must accompany
the Minimal Corresponding Source and Corresponding Application
Code. If you use option 4d1, you must provide the Installation
Information in the manner specified by section 6 of the GNU GPL
for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the
Library side by side in a single library together with other library
facilities that are not Applications and are not
covered by this
License, and convey such a combined library under terms of your
choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based
on the Library, uncombined with any other library facilities,
conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it
is a work based on the Library, and explaining where to find the
accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions
of the GNU Lesser General Public License from time to time. Such new
versions will be similar in spirit to the present version, but may
differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the
Library as you received it specifies that a certain numbered version
of the GNU Lesser General Public License "or
any later version"
applies to it, you have the option of following the terms and
conditions either of that published version or of any later version
published by the Free Software Foundation. If the Library as you
received it does not specify a version number of the GNU Lesser
General Public License, you may choose any version of the GNU Lesser
General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide
whether future versions of the GNU Lesser General Public License shall
apply, that proxy's public statement of acceptance of any version is
permanent authorization for you to choose that version for the
Library.
COPYING.other -*- org -*-
#+TITLE: List of code with permissive licenses as used by GnuPG.
#+STARTUP: showall

* DNS resolver (dirmngr/dns.c)

dns.c - Recursive, Reentrant DNS Resolver.

Copyright (c) 2008, 2009, 2010, 2012-2016 William Ahern

Permission is hereby granted, free of charge, to any person obtaining a
copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to permit
persons to whom the Software is furnished to do so, subject to the
following conditions:

The above copyright notice and this permission notice shall be included
in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY
OF ANY KIND, EXPRESS
OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN
NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM,
DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR
OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE
USE OR OTHER DEALINGS IN THE SOFTWARE.

* TinySCHEME (tests/gpgscm/LICENSE.TinySCHEME)

Copyright (c) 2000, Dimitrios Souflis
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are
met:

Redistributions of source code must retain the above copyright notice,
this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided
with the distribution.

Neither the name of Dimitrios Souflis nor the names of the
contributors may be used to endorse or promote products derived from
this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,

EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

1.49 harfbuzz 1.3.0

1.49.1 Available under license :

HarfBuzz is licensed under the so-called "Old MIT" license. Details follow.
For parts of HarfBuzz that are licensed under different licenses see individual
files names COPYING in subdirectories where applicable.

Copyright 2010,2011,2012,2013,2014,2015,2016,2017,2018,2019 Google, Inc.
Copyright 2019 Facebook, Inc.
Copyright 2012 Mozilla Foundation
Copyright 2011 Codethink Limited
Copyright 2008,2010 Nokia Corporation and/or its subsidiary(-ies)
Copyright 2009 Keith Stribley
Copyright 2009 Martin Hosken and SIL International
Copyright 2007 Chris Wilson
Copyright 2006 Behdad Esfahbod
Copyright 2005 David Turner
Copyright 2004,2007,2008,2009,2010 Red Hat, Inc.
Copyright 1998-2004 David Turner and Werner Lemberg

For full copyright notices consult the individual files in the package.

Permission is hereby granted, without written agreement and without
license or royalty fees, to use, copy, modify, and distribute this
software and its documentation for any purpose,
 provided that the
above copyright notice and the following two paragraphs appear in
all copies of this software.

IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE TO ANY PARTY FOR
DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES
ARISING OUT OF THE USE OF THIS SOFTWARE AND ITS DOCUMENTATION, EVEN
IF THE COPYRIGHT HOLDER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH
DAMAGE.

THE COPYRIGHT HOLDER SPECIFICALLY DISCLAIMS ANY WARRANTIES, INCLUDING,
BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND
FITNESS FOR A PARTICULAR PURPOSE. THE SOFTWARE PROVIDED HEREUNDER IS
ON AN "AS IS" BASIS, AND THE COPYRIGHT HOLDER HAS NO OBLIGATION TO

PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.
The following license applies to many of the fonts in this folder.

This Font Software is licensed under the SIL Open Font License,
Version 1.1.

This license is copied below, and is also available with a FAQ at:
http://scripts.sil.org/OFL

SIL OPEN FONT LICENSE Version 1.1 - 26 February 2007

PREAMBLE
The goals of the Open Font License (OFL) are to stimulate worldwide
development of collaborative font projects, to support the font
creation efforts of academic and linguistic communities, and to
provide a free and open framework in which fonts may be shared and
improved in partnership with others.

The OFL allows the licensed fonts to be used, studied, modified and
redistributed freely as long as they are not sold by themselves. The
fonts, including any derivative works, can be bundled, embedded,
redistributed and/or sold with any software provided that any reserved
names
are not used by derivative works. The fonts and derivatives,
however, cannot be released under any other type of license. The
requirement for fonts to remain under this license does not apply to
any document created using the fonts or their derivatives.

DEFINITIONS
"Font Software" refers to the set of files released by the Copyright
Holder(s) under this license and clearly marked as such. This may
include source files, build scripts and documentation.

"Reserved Font Name" refers to any names specified as such after the
copyright statement(s).

"Original Version" refers to the collection of Font Software
components as distributed by the Copyright Holder(s).

"Modified Version" refers to any derivative made by adding to,
deleting, or substituting -- in part or in whole -- any of the
components of the Original Version, by changing formats or by porting
the Font Software to a new environment.

"Author" refers to any designer, engineer, programmer, technical

writer or other person who
contributed to the Font Software.

PERMISSION & CONDITIONS
Permission is hereby granted, free of charge, to any person obtaining
a copy of the Font Software, to use, study, copy, merge, embed,
modify, redistribute, and sell modified and unmodified copies of the
Font Software, subject to the following conditions:

1) Neither the Font Software nor any of its individual components, in
Original or Modified Versions, may be sold by itself.

2) Original or Modified Versions of the Font Software may be bundled,
redistributed and/or sold with any software, provided that each copy
contains the above copyright notice and this license. These can be
included either as stand-alone text files, human-readable headers or
in the appropriate machine-readable metadata fields within text or
binary files as long as those fields can be easily viewed by the user.

3) No Modified Version of the Font Software may use the Reserved Font
Name(s) unless explicit written permission is granted by the
corresponding
Copyright Holder. This restriction only applies to the
primary font name as presented to the users.

4) The name(s) of the Copyright Holder(s) or the Author(s) of the Font
Software shall not be used to promote, endorse or advertise any
Modified Version, except to acknowledge the contribution(s) of the
Copyright Holder(s) and the Author(s) or with their explicit written
permission.

5) The Font Software, modified or unmodified, in part or in whole,
must be distributed entirely under this license, and must not be
distributed under any other license. The requirement for fonts to
remain under this license does not apply to any document created using
the Font Software.

TERMINATION
This license becomes null and void if any of the above conditions are
not met.

DISCLAIMER
THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT
OF COPYRIGHT, PATENT,
TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL THE
COPYRIGHT HOLDER BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY,

INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.
Copyright 2016 Unicode Inc. All rights reserved.

Licensed under the Apache License, Version2.0 (the License);
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an AS IS BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
CC BY-NC-SA 3.0
http://www.crulp.org/software/license/CreativeCommons.html
https://creativecommons.org/licenses/by-nc-sa/3.0/
Copyright 2000-2016 Adobe Systems Incorporated. All Rights Reserved.

Licensed under the Apache License, Version 2.0 (the "License");
you may not use these files except in compliance with the License.
You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
Copyright (c) 2010 Red Hat Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE

AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.

1.50 bash 4.3.47

1.50.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it. (Some other Free Software Foundation software is covered by
the GNU Lesser General Public License instead.) You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price. Our General Public Licenses are designed
to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid
anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate to certain responsibilities for you if you
distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether
gratis or for a fee, you must give the recipients all the rights that
you have. You must make sure that they, too, receive or can get the
source code. And you must show them these terms so they know their
rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute
and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which
contains
a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies
of the Program's
source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the

notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole
or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered
independent and separate works in
themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it,
under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or
executable form with such
an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the
source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt

otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made

generous contributions to the wide range of software distributed
through that system in reliance on consistent application of that
system; it is up to the author/donor to decide if he or she is willing
to distribute software through
 any other system and a licensee cannot
impose that choice.

This section is intended to make thoroughly clear what is believed to
be a consequence of the rest of this License.

 8. If the distribution and/or use of the Program is restricted in
certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Program under this License
may add an explicit geographical distribution limitation excluding
those countries, so that distribution is permitted only in or among
countries not thus excluded. In such case, this License incorporates
the limitation as if written in the body of this License.

 9. The Free Software Foundation may publish revised and/or new versions
of the General Public License from time to time. Such new versions will
be similar in spirit to the present version, but may differ in detail to
address new problems or concerns.

Each version is given a distinguishing version number. If the Program
specifies a version number
 of this License which applies to it and "any
later version", you have the option of following the terms and conditions
either of that version or of any later version published by the Free
Software Foundation. If the Program does not specify a version number of
this License, you may choose any version ever published by the Free Software
Foundation.

 10. If you wish to incorporate parts of the Program into other free
programs whose distribution conditions are different, write to the author
to ask for permission. For software which is copyrighted by the Free
Software Foundation, write to the Free Software Foundation; we sometimes
make exceptions for this. Our decision will be guided by the two goals
of preserving the free status of all derivatives of our free software and
of promoting the sharing and reuse of software generally.

NO WARRANTY

 11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY
FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW.
 EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES
PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED
OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF

MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN
IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License,
or
(at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

```
Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.
```

The hypothetical commands `show w'
and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

```
Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice
```

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this is what you want to do, use the GNU Lesser General
Public License instead of this License.

GNU Free Documentation License
Version 1.3, 3 November 2008

Copyright (C) 2000, 2001, 2002, 2007, 2008 Free Software Foundation, Inc.
<http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other
functional and useful document "free" in the sense of freedom: to
assure everyone the effective freedom to copy and redistribute it,
with or without modifying it, either commercially or noncommercially.
Secondarily, this License preserves for the author and publisher a way
to get credit for their work, while not being considered responsible

for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections,

in the notice
that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters
or
for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some
word
processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

The "publisher" means any person or entity that distributes copies of the Document to the public.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The
Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section
3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.
E. Add an appropriate copyright notice for your modifications
adjacent to the other copyright notices.
F. Include, immediately after the copyright notices, a license notice
giving the public permission to use the Modified Version under the
terms of this License, in the form shown in the Addendum below.
G. Preserve in that license notice the full lists of Invariant Sections
and required Cover Texts given in the Document's license notice.
H. Include an unaltered copy of this License.
I. Preserve the section Entitled "History", Preserve its Title, and add
to it an item stating at least the title, year,
new authors, and
publisher of the Modified Version as given on the Title Page. If
there is no section Entitled "History" in the Document, create one
stating the title, year, authors, and publisher of the Document as
given on its Title Page, then add an item describing the Modified
Version as stated in the previous sentence.
J. Preserve the network location, if any, given in the Document for
public access to a Transparent copy of the Document, and likewise
the network locations given in the Document for previous versions
it was based on. These may be placed in the "History" section.
You may omit a network location for a work that was published at
least four years before the Document itself, or if the original
publisher of the version it refers to gives permission.
K. For any section Entitled "Acknowledgements" or "Dedications",
Preserve the Title of the section, and preserve in the section all
the substance and tone of each of the contributor
acknowledgements
and/or dedications given therein.
L. Preserve all the Invariant Sections of the Document,
unaltered in their text and in their titles. Section numbers
or the equivalent are not considered part of the section titles.
M. Delete any section Entitled "Endorsements". Such a section
may not be included in the Modified Version.
N. Do not retitle any existing section to be Entitled "Endorsements"
or to conflict in title with any Invariant Section.
O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or
appendices that qualify as Secondary Sections and contain no material
copied from the Document, you may at your option designate some or all
of these sections as invariant. To do this, add their titles to the
list of Invariant Sections in the Modified Version's license notice.
These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains
nothing but

endorsements of your Modified Version by various
parties--for example, statements of peer review or that the text has
been approved by an organization as the authoritative definition of a
standard.

You may add a passage of up to five words as a Front-Cover Text, and a
passage of up to 25 words as a Back-Cover Text, to the end of the list
of Cover Texts in the Modified Version. Only one passage of
Front-Cover Text and one of Back-Cover Text may be added by (or
through arrangements made by) any one entity. If the Document already
includes a cover text for the same cover, previously added by you or
by arrangement made by the same entity you are acting on behalf of,
you may not add another; but you may replace the old one, on explicit
permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License
give permission to use their names for publicity for or to assert or
imply endorsement of any Modified Version.

5. COMBINING
DOCUMENTS

You may combine the Document with other documents released under this
License, under the terms defined in section 4 above for modified
versions, provided that you include in the combination all of the
Invariant Sections of all of the original documents, unmodified, and
list them all as Invariant Sections of your combined work in its
license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and
multiple identical Invariant Sections may be replaced with a single
copy. If there are multiple Invariant Sections with the same name but
different contents, make the title of each such section unique by
adding at the end of it, in parentheses, the name of the original
author or publisher of that section if known, or else a unique number.
Make the same adjustment to the section titles in the list of
Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections
Entitled "History"
in the various original documents, forming one section Entitled
"History"; likewise combine any sections Entitled "Acknowledgements",
and any sections Entitled "Dedications". You must delete all sections
Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives
with other separate
and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under
the terms of section 4.
Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions

of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

11. RELICENSING

"Massive Multiauthor Collaboration Site" (or "MMC Site") means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A "Massive Multiauthor Collaboration" (or "MMC") contained in the site means any set of copyrightable works thus published on the MMC site.

"CC-BY-SA" means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

"Incorporate" means to publish or republish a Document, in whole or in part, as part of another Document.

An MMC is "eligible for relicensing" if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and

license notices just after the title page:

```
  Copyright (c)  YEAR  YOUR NAME.
  Permission is granted to copy, distribute and/or modify this document
   under the terms of the GNU Free Documentation License, Version 1.3
  or any later version published by the Free Software Foundation;
  with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
  A copy of the license is included in the section entitled "GNU
  Free Documentation License".
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts,
replace the "with...Texts." line with this:

```
  with the Invariant Sections being LIST THEIR TITLES, with the
  Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.
```

If you have Invariant Sections without Cover Texts, or some other
combination of the three, merge those two alternatives to suit the
situation.

If your document contains nontrivial examples of program code, we
recommend releasing these examples in parallel under your choice of
free software license, such as the GNU General Public License,
to permit their use in free software.
@c The GNU Free Documentation License.
@center Version 1.3, 3 November 2008

@c This file is intended to be included within another document,
@c hence no sectioning command or @node.

@display
Copyright @copyright{} 2000, 2001, 2002, 2007, 2008 Free Software Foundation, Inc.
@uref{http://fsf.org/}

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.
@end display

@enumerate 0
@item
PREAMBLE

The purpose of this License is to make a manual, textbook, or other
functional and useful document @dfn{free} in the sense of freedom: to
assure everyone the effective freedom to copy and redistribute it,
with or without modifying it, either commercially or noncommercially.
Secondarily, this License preserves for the author and publisher a way
to get credit for their work, while not being considered responsible

for modifications made by others.

This License is a kind of ``copyleft'', which means that derivative works of the document
must themselves be free in the same sense. It
complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

@item
APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The ``Document'', below, refers
to any such manual or work. Any member of the public is a licensee, and is addressed as ``you''. You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A ``Modified Version'' of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A ``Secondary Section'' is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political
position regarding
them.

The ``Invariant Sections'' are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice

that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The ``Cover Texts'' are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A ``Transparent'' copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not ``Transparent'' is called ``Opaque''.

Examples of suitable formats for Transparent copies include plain @sc{ascii} without markup, Texinfo input format, La@TeX{} input format, @acronym{SGML} or @acronym{XML} using a publicly available @acronym{DTD}, and standard-conforming simple @acronym{HTML}, PostScript or @acronym{PDF} designed for human modification. Examples of transparent image formats include @acronym{PNG}, @acronym{XCF} and @acronym{JPG}. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, @acronym{SGML} or @acronym{XML} for which the @acronym{DTD} and/or processing tools are not generally available, and the machine-generated @acronym{HTML}, PostScript or @acronym{PDF} produced by some word processors for output purposes only.

The ``Title Page'' means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, ``Title Page'' means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

The ``publisher'' means any person or entity that distributes copies of the Document to the public.

A section ``Entitled XYZ'' means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in
another language. (Here XYZ stands for a
specific section name mentioned below, such as ``Acknowledgements'', ``Dedications'', ``Endorsements'', or ``History''.) To ``Preserve the Title'' of such a section when you modify the Document means that it remains a section ``Entitled XYZ'' according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

@item
VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever
to those of this License. You may not use
technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

@item
COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible.
You may add other material on the covers in addition.
Copying with changes limited to the covers, as long as they preserve

the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that
this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

@item
MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

@enumerate A
@item
Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from
those of previous versions
(which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

@item
List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified

Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

@item
State on the Title page the name of the publisher of the Modified Version, as the publisher.

@item
Preserve all the copyright notices of the Document.

@item
Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

@item
Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in
the Addendum below.

@item
Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

@item
Include an unaltered copy of this License.

@item
Preserve the section Entitled ``History'', Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled ``History'' in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

@item
Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the ``History'' section. You may omit a network location for a work that was published at least
four years before the Document itself, or if the original publisher of the version it refers to gives permission.

@item

For any section Entitled ``Acknowledgements'' or ``Dedications'', Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

@item
Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

@item
Delete any section Entitled ``Endorsements''. Such a section may not be included in the Modified Version.

@item
Do not retitle any existing section to be Entitled ``Endorsements'' or to conflict in title with any Invariant Section.

@item
Preserve any Warranty Disclaimers.
@end enumerate

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document,
you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled ``Endorsements'', provided it contains nothing but endorsements of your Modified Version by various parties---for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of,
you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License

give permission to use their names for publicity for or to assert or
imply endorsement of any Modified Version.

@item
COMBINING DOCUMENTS

You may combine the Document with other documents released under this
License, under the terms defined in section 4 above for modified
versions, provided that you include in the combination all of the
Invariant Sections of all of the original documents, unmodified, and
list them all as Invariant Sections of your combined work in its
license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and
multiple identical Invariant Sections may be replaced with a single
copy. If there are multiple Invariant Sections with the same name but
different contents, make the title of
 each such section unique by
adding at the end of it, in parentheses, the name of the original
author or publisher of that section if known, or else a unique number.
Make the same adjustment to the section titles in the list of
Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled ``History"
in the various original documents, forming one section Entitled
``History"; likewise combine any sections Entitled ``Acknowledgements",
and any sections Entitled ``Dedications". You must delete all
sections Entitled ``Endorsements."

@item
COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents
released under this License, and replace the individual copies of this
License in the various documents with a single copy that is included in
the collection, provided that you follow the rules of this License for
verbatim copying of each of the documents in all other respects.

You may extract
 a single document from such a collection, and distribute
it individually under this License, provided you insert a copy of this
License into the extracted document, and follow this License in all
other respects regarding verbatim copying of that document.

@item
AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate

and independent documents or works, in or on a volume of a storage or distribution medium, is called an ``aggregate'' if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may
be placed on
covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

@item
TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original
version will prevail.

If a section in the Document is Entitled ``Acknowledgements'', ``Dedications'', or ``History'', the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

@item
TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license

from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

@item
FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See @uref{http://www.gnu.org/copyleft/}.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License ``or any later version'' applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

@item
RELICENSING

``Massive Multiauthor Collaboration Site'' (or ``MMC Site'') means any World Wide Web server that publishes copyrightable works and also

provides prominent facilities for anybody to edit those works. A
public wiki that anybody can edit is an example of such a server. A
``Massive Multiauthor Collaboration'' (or ``MMC'')
contained in the
site means any set of copyrightable works thus published on the MMC
site.

``CC-BY-SA'' means the Creative Commons Attribution-Share Alike 3.0
license published by Creative Commons Corporation, a not-for-profit
corporation with a principal place of business in San Francisco,
California, as well as future copyleft versions of that license
published by that same organization.

``Incorporate'' means to publish or republish a Document, in whole or
in part, as part of another Document.

An MMC is ``eligible for relicensing'' if it is licensed under this
License, and if all works that were first published under this License
somewhere other than this MMC, and subsequently incorporated in whole
or in part into the MMC, (1) had no cover texts or invariant sections,
and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site
under CC-BY-SA on the same site at any time before August 1, 2009,
provided the
MMC is eligible for relicensing.

@end enumerate

@page
@heading ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of
the License in the document and put the following copyright and
license notices just after the title page:

@smallexample
@group
Copyright (C) @var{year} @var{your name}.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.3
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover
Texts. A copy of the license is included in the section entitled ``GNU
Free Documentation License''.
@end group
@end smallexample

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts,
replace the ``with@dots{}Texts." line with this:

@smallexample
@group
  with the Invariant Sections being @var{list their titles}, with
  the Front-Cover
Texts being @var{list}, and with the Back-Cover Texts
  being @var{list}.
@end group
@end smallexample

If you have Invariant Sections without Cover Texts, or some other
combination of the three, merge those two alternatives to suit the
situation.

If your document contains nontrivial examples of program code, we
recommend releasing these examples in parallel under your choice of
free software license, such as the GNU General Public License,
to permit their use in free software.

@c Local Variables:
@c ispell-local-pdict: "ispell-dict"
@c End:

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for
software and other kinds of works.

The licenses for most software and other practical works are designed
to take away your freedom to share and change the works. By contrast,
the GNU General Public License is intended to guarantee your freedom to
share and change all versions of a program--to make sure it remains free
software for all its users. We, the Free Software Foundation, use the
GNU General Public License for most of our software; it applies also to
any other work released this way by its authors. You can apply it to
your programs, too.

When we speak of free software, we are referring to
freedom, not
price. Our General Public Licenses are designed to make sure that you

have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1)
assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand
ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source

form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered

by this License only if the output, given its
content, constitutes a covered work. This License acknowledges your
rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not
convey, without conditions so long as your license otherwise remains
in force. You may convey covered works to others for the sole purpose
of having them make modifications exclusively for you, or provide you
with facilities for running those works, provided that you comply with
the terms of this License in conveying all material for which you do
not control copyright. Those thus making or running the covered works
for you must do so exclusively on your behalf, under your direction
and control, on terms that prohibit them from making any copies of
your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under
the conditions stated below. Sublicensing is not allowed;
section 10
makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological
measure under any applicable law fulfilling obligations under article
11 of the WIPO copyright treaty adopted on 20 December 1996, or
similar laws prohibiting or restricting circumvention of such
measures.

When you convey a covered work, you waive any legal power to forbid
circumvention of technological measures to the extent such circumvention
is effected by exercising rights under this License with respect to
the covered work, and you disclaim any intention to limit operation or
modification of the work as a means of enforcing, against the work's
users, your or third parties' legal rights to forbid circumvention of
technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you
receive it, in any medium, provided that you conspicuously and
appropriately
publish on each copy an appropriate copyright notice;
keep intact all notices stating that this License and any
non-permissive terms added in accord with section 7 apply to the code;
keep intact all notices of the absence of any warranty; and give all
recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey,

and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization
keys, or other information required to install
and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in
ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on

those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above
requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright
holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights
granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted

by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered

work if you are a party to an arrangement with a third party that is
in the business of distributing software, under which you make payment
to the third party based on the extent of your activity of conveying
the work, and under which the third party grants, to any of the
parties who would receive the covered work from you, a discriminatory
patent license (a) in connection with copies of the covered work
conveyed by you (or copies made from those copies), or (b) primarily
for and in connection with specific products or compilations that
contain the covered work, unless you entered into that arrangement,
or
that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting
any implied license or other defenses to infringement that may
otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or
otherwise) that contradict the conditions of this License, they do not
excuse you from the conditions of this License. If you cannot convey a
covered work so as to satisfy simultaneously your obligations under this
License and any other pertinent obligations, then as a consequence you may
not convey it at all. For example, if you agree to terms that obligate you
to collect a royalty for further conveying from those to whom you convey
the Program, the only way you could satisfy both those terms and this
License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have
permission to link or combine any covered work with a work licensed
under version 3 of the GNU Affero General Public License into a single
combined work, and to convey the resulting work. The terms of this
License will continue to apply to the part which is the covered work,
but the special requirements of the GNU Affero General Public License,
section 13, concerning interaction through a network will apply to the
combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of
the GNU General Public License from time to time. Such new versions will
be similar in spirit to the present version, but may differ in detail to
address new problems or concerns.

Each version is given a distinguishing version number. If the
Program specifies that a certain numbered version of the GNU General

Public License "or any later version" applies to it, you have the
option of following the terms and conditions either of that numbered
version or of any later version published by the Free Software
Foundation. If the Program does not specify a version number of the
GNU General Public License, you may choose any version ever published
by the Free Software Foundation.

If the Program specifies that a proxy can decide which future
versions of the GNU General Public License can be used, that proxy's
public statement of acceptance of a version permanently authorizes you
to choose that version for the Program.

Later license versions may give you additional or different
permissions. However, no additional obligations are imposed on any
author or copyright holder as a result of your choosing to follow a
later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY
APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT
HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY
OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM
IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF
ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING
WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS
THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY
GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE
USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF
DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD
PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS),
EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF
SUCH DAMAGES.

17.
Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided
above cannot be given local legal effect according to their terms,
reviewing courts shall apply local law that most closely approximates

an absolute waiver of all civil liability in connection with the
Program, unless a warranty or assumption of liability accompanies a
copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest
possible use to the public, the best way to achieve this is to make it
free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest
to attach them to the start of each source file to most effectively
state the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where
the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation, either version 3 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>
This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what you want to
do, use the GNU Lesser General
Public License instead of this License. But first, please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.
Unless otherwise stated, all files in this directory are Copyright (C)
1991,1992,1993,1994,1995,1996,1997,1998,1999,2000,2001,2002,2003,
2004,2005,2006,2007,2008,2009,2010,2011
Free Software Foundation, Inc.

See the file COPYING in the bash distribution root directory for copying
and usage restrictions.

The file ifs-posix.tests is Copyright (C) 2005 Glen Fowler.

1.51 cairo 1.14.6

1.51.1 Available under license :

Cairo is free software.

cairo-trace is released under the terms of the GNU General Public License
(GPL) version 3. Please see COPYING-GPL-3 for the precise terms and
conditions.
GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to

using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed
to make sure that you
have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute
and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which

contains
a notice placed by the copyright holder saying it may be distributed
under the terms of this General Public License. The "Program", below,
refers to any such program or work, and a "work based on the Program"
means either the Program or any derivative work under copyright law:
that is to say, a work containing the Program or a portion of it,
either verbatim or with modifications and/or translated into another
language. (Hereinafter, translation is included without limitation in
the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not
covered by this License; they are outside its scope. The act of
running the Program is not restricted, and the output from the Program
is covered only if its contents constitute a work based on the
Program (independent of having been made by running the Program).
Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies
of the Program's
source code as you receive it, in any medium, provided that you
conspicuously and appropriately publish on each copy an appropriate
copyright notice and disclaimer of warranty; keep intact all the
notices that refer to this License and to the absence of any warranty;
and give any other recipients of the Program a copy of this License
along with the Program.

You may charge a fee for the physical act of transferring a copy, and
you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion
of it, thus forming a work based on the Program, and copy and
distribute such modifications or work under the terms of Section 1
above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices
stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in
whole
or in part contains or is derived from the Program or any
part thereof, to be licensed as a whole at no charge to all third
parties under the terms of this License.

c) If the modified program normally reads commands interactively
when run, you must cause it, when started running for such
interactive use in the most ordinary way, to print or display an
announcement including an appropriate copyright notice and a
notice that there is no warranty (or else, saying that you provide

a warranty) and that users may redistribute the program under
these conditions, and telling the user how to view a copy of this
License. (Exception: if the Program itself is interactive but
does not normally print such an announcement, your work based on
the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If
identifiable sections of that work are not derived from the Program,
and can be reasonably considered
independent and separate works in
themselves, then this License, and its terms, do not apply to those
sections when you distribute them as separate works. But when you
distribute the same sections as part of a whole which is a work based
on the Program, the distribution of the whole must be on the terms of
this License, whose permissions for other licensees extend to the
entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest
your rights to work written entirely by you; rather, the intent is to
exercise the right to control the distribution of derivative or
collective works based on the Program.

In addition, mere aggregation of another work not based on the Program
with the Program (or with a work based on the Program) on a volume of
a storage or distribution medium does not bring the other work under
the scope of this License.

3. You may copy and distribute the Program (or a work based
on it,
under Section 2) in object code or executable form under the terms of
Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable
source code, which must be distributed under the terms of Sections
1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three
years, to give any third party, for a charge no more than your
cost of physically performing source distribution, a complete
machine-readable copy of the corresponding source code, to be
distributed under the terms of Sections 1 and 2 above on a medium
customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer
to distribute corresponding source code. (This alternative is
allowed only for noncommercial distribution and only if you
received the program in object code or

executable form with such
an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the
source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each
time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent

infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number

of this License which applies to it and "any
later version", you have the option of following the terms and conditions
either of that version or of any later version published by the Free
Software Foundation. If the Program does not specify a version number of
this License, you may choose any version ever published by the Free Software
Foundation.

10. If you wish to incorporate parts of the Program into other free
programs whose distribution conditions are different, write to the author
to ask for permission. For software which is copyrighted by the Free
Software Foundation, write to the Free Software Foundation; we sometimes
make exceptions for this. Our decision will be guided by the two goals
of preserving the free status of all derivatives of our free software and
of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY
FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW.
EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES
PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED
OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS
TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE
PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING,
REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING
WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR
REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES,
INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING
OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED
TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY
YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER
PROGRAMS), EVEN
IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE
POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest
possible use to the public, the best way to achieve this is to make it
free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest

to attach them to the start of each source file to most effectively
convey the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where the full notice is found.

  <one line to give the program's name and a brief idea of what it does.>
  Copyright (C) <year> <name of author>

  This program is free software; you can redistribute it and/or modify
  it under the terms of the GNU General Public License as published by
  the Free Software Foundation; either version 2 of the License,
or
  (at your option) any later version.

  This program is distributed in the hope that it will be useful,
  but WITHOUT ANY WARRANTY; without even the implied warranty of
  MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
  GNU General Public License for more details.

  You should have received a copy of the GNU General Public License
  along with this program; if not, write to the Free Software
  Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

  Gnomovision version 69, Copyright (C) year name of author
  Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
  This is free software, and you are welcome to redistribute it
  under certain conditions; type `show c' for details.

The hypothetical commands `show
 w' and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

 Yoyodyne, Inc., hereby disclaims all copyright interest in the program
 `Gnomovision' (which makes passes at compilers) written by James Hacker.

 <signature of Ty Coon>, 1 April 1989
 Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin Street, Suite 500, Boston, MA 02110-1335, USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library,
whether gratis
or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software
patents pose a constant threat to the existence of
any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits
such linking only if the
entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages

are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under

copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into
another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any
medium, provided that
you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the
terms of this License.

d) If a facility in the modified Library refers to a function or a

table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can
be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the
ordinary GNU General Public
License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all

subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the

object code for the work under the terms of Section 6.
Any executables containing that work also fall under Section 6,
whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or
link a "work that uses the Library" with the Library to produce a
work containing portions of the Library, and distribute that work
under terms of your choice, provided that the terms permit
modification of the work for the customer's own use and reverse
engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the
Library is used in it and that the Library and its use are covered by
this License. You must supply a copy of this License. If the work
during execution displays copyright notices, you must include the
copyright notice for the Library among them, as well as a reference
directing the user to the copy of this License. Also, you must do one
of these things:

a) Accompany
the work with the complete corresponding
machine-readable source code for the Library including whatever
changes were used in the work (which must be distributed under
Sections 1 and 2 above); and, if the work is an executable linked
with the Library, with the complete machine-readable "work that
uses the Library", as object code and/or source code, so that the
user can modify the Library and then relink to produce a modified
executable containing the modified Library. (It is understood
that the user who changes the contents of definitions files in the
Library will not necessarily be able to recompile the application
to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the
Library. A suitable mechanism is one that (1) uses at run time a
copy of the library already present on the user's computer system,
rather than copying library functions into the executable, and (2)
will operate
properly with a modified version of the library, if
the user installs one, as long as the modified version is
interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least
three years, to give the same user the materials specified in
Subsection 6a, above, for a charge no more than the cost of
performing this distribution.

d) If distribution of the work is made by offering access to copy
from a designated place, offer equivalent access to copy the above

specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally
distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with
any other library
facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or

distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to

be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY

AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE,
BE LIABLE TO YOU
FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively
convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Suite 500, Boston, MA 02110-1335, USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or
your school, if any, to sign a "copyright disclaimer" for the library,
if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the
library `Frob' (a library for tweaking knobs) written by James
Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!
Cairo is free software.

These tests are mainly available under a liberal MIT license to simplify
any use of the code for reference purposes. Please check the opening comment
of each file for copyright and licensing information.

The test suite also bundles some fonts for use by the test suite. The
fonts included, their licenses, and why we use them in the test suite
are as follows:

Font	License	Distinguishing feature
6x13.pcf	Public Domain	Bitmap font

The test suite also bundles some images for use by the test suite. The
images included, their licenses, and why we use them in the test suite
are as follows:

Image	License	Distinguishing feature
romedalen.jpg	Public Domain	Bitmap image (image/jpeg)
romedalen.png	Public Domain	Bitmap image (image/png)

The kind contributors of the bundled files are (in alphabetical order):
yvind Kols <pippin@freedesktop.org> Author of the original
romedalen shot.
Cairo is free software.

Every source file in the implementation of cairo is available to be
redistributed and/or modified under the terms of either the GNU Lesser
General Public License (LGPL) version 2.1 or the Mozilla Public
License (MPL) version 1.1. Some files are available under more
liberal terms, but we believe that in all cases, each file may be used
under either the LGPL or the MPL.

See the following files in this directory for the precise terms and
conditions of either license:

COPYING-LGPL-2.1
COPYING-MPL-1.1

Please see each file in the implementation for copyright and licensing
information, (in the opening comment of each file).

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for
software and other kinds of works.

The licenses for most software and other practical works are designed
to take away your freedom to share and change the works. By contrast,
the GNU General Public License is intended to guarantee your freedom to
share and change all versions of a program--to make sure it remains free
software for all its users. We, the Free Software Foundation, use the
GNU General Public License for most of our software; it applies also to
any other work released this way by its authors. You can apply it to
your programs, too.

When we speak of free software, we are referring to
freedom, not
price. Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
them if you wish), that you receive source code or can get it if you
want it, that you can change the software or use pieces of it in new
free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you
these rights or asking you to surrender the rights. Therefore, you have
certain responsibilities if you distribute copies of the software, or if
you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether
gratis or for a fee, you must pass on to the recipients the same
freedoms that you received. You must make sure that they, too, receive
or can get the source code. And you must show them these terms so they
know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work

in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system

(if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed;

section 10
makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately
publish on each copy an appropriate copyright notice;
keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this
License to anyone who comes into possession of a copy. This
License will therefore apply, along with any applicable section 7
additional terms, to the whole of the work, and all its parts,
regardless of how they are packaged. This License gives no
permission to license the work in any other way, but it does not
invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display
Appropriate Legal Notices; however, if the Program has interactive
interfaces that do not display Appropriate Legal Notices, your
work need not make them do so.

A compilation of a covered work with other separate and independent
works, which are not by their nature extensions of the covered work,
and which are not combined with it such as to form a larger program,
in or on a volume of a storage or distribution
medium, is called an
"aggregate" if the compilation and its resulting copyright are not
used to limit the access or legal rights of the compilation's users
beyond what the individual works permit. Inclusion of a covered work
in an aggregate does not cause this License to apply to the other
parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms
of sections 4 and 5, provided that you also convey the
machine-readable Corresponding Source under the terms of this License,
in one of these ways:

a) Convey the object code in, or embodied in, a physical product
(including a physical distribution medium), accompanied by the
Corresponding Source fixed on a durable physical medium
customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product
(including a physical distribution medium), accompanied by a
written offer, valid for at least three years
and valid for as
long as you offer spare parts or customer support for that product
model, to give anyone who possesses the object code either (1) a
copy of the Corresponding Source for all the software in the
product that is covered by this License, on a durable physical
medium customarily used for software interchange, for a price no
more than your reasonable cost of physically performing this
conveying of source, or (2) access to copy the
Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in
the same way through the same place at no
further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source
as a System Library, need not be
included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization
keys, or other information required to install
and execute modified versions of a covered work in that User Product from

a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in
ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the
entire Program shall
be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work,

for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on

those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions;

the above
requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright
holder, and you cure the violation prior to 30 days after
your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and

propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights
granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For
purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a

party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the
option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY
OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17.
Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where

the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation, either version 3 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>
This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what you want to
do, use the GNU Lesser General
Public License instead of this License. But first, please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.
Cairo is free software.

These utilities are all free software, please see the licensing conditions

in the opening comments of each file.
Cairo is free software.

Every source file in the implementation[*] of cairo is available to be
redistributed and/or modified under the terms of either the GNU Lesser
General Public License (LGPL) version 2.1 or the Mozilla Public
License (MPL) version 1.1. Some files are available under more
liberal terms, but we believe that in all cases, each file may be used
under either the LGPL or the MPL.

See the following files in this directory for the precise terms and
conditions of either license:

COPYING-LGPL-2.1
COPYING-MPL-1.1

Please see each file in the implementation for copyright and licensing
information, (in the opening comment of each file).

[*] The implementation of cairo is contained entirely within the "src"
directory of the cairo source distribution. There are other components
of the cairo source distribution (such as the "test", "util", and "perf")
that are auxiliary to the library itself. None of the source code in these
directories contributes to a build of the cairo library
itself, (libcairo.so
or cairo.dll or similar).

These auxiliary components are also free software, but may be under
different license terms than cairo itself. For example, most of the
test cases in the perf and test directories are made available under
an MIT license to simplify any use of this code for reference purposes
in using cairo itself. Other files might be available under the GNU
General Public License (GPL), for example. Again, please see the COPYING
file under each directory and the opening comment of each file for copyright
and licensing information.
Cairo is free software.

These tests are mainly available under a liberal MIT license to simplify
any use of the code for reference purposes. Please check the opening comment
of each file for copyright and licensing information.

MOZILLA PUBLIC LICENSE
Version 1.1

---

1. Definitions.

1.0.1. "Commercial Use" means distribution or otherwise making the

Covered Code available to a third party.

1.1. "Contributor" means each entity that creates or contributes to the creation of Modifications.

1.2. "Contributor Version" means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.

1.3. "Covered Code" means the Original Code or Modifications or the combination of the Original Code and Modifications, in each case including portions thereof.

1.4. "Electronic Distribution Mechanism" means a mechanism generally accepted in the software development community for the electronic transfer of data.

1.5. "Executable" means Covered Code in any form other than Source Code.

1.6. "Initial Developer" means the individual or entity identified as the Initial Developer in the Source Code notice required by Exhibit A.

1.7. "Larger Work" means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.

1.8. "License" means this document.

1.8.1. "Licensable" means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9. "Modifications" means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:

A. Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.

B. Any new file that contains any part of the Original Code or previous Modifications.

1.10. "Original Code" means Source Code of computer software code which is described in the Source Code notice required by Exhibit A as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.

1.10.1. "Patent Claims" means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1.11. "Source Code" means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor's choice. The Source Code can be in a compressed or
archival form, provided the
appropriate decompression or de-archiving software is widely available for no charge.

1.12. "You" (or "Your") means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6.1. For legal entities, "You" includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. Source Code License.

2.1. The Initial Developer Grant.
The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property

claims:

(a) under intellectual property rights (other than patent or trademark) Licensable by Initial Developer to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, and/or as part of a Larger Work; and

(b) under Patents Claims infringed by the making, using or selling of Original Code, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Code (or portions thereof).

(c) the licenses granted in this Section 2.1(a) and (b) are effective on the date Initial Developer first distributes Original Code under the terms of this License.

(d) Notwithstanding Section 2.1(b) above, no patent license is granted: 1) for code that You delete from the Original Code; 2) separate from the Original Code; or 3) for infringements caused by: i) the modification of the Original Code or ii) the combination of the Original Code with other software or devices.

2.2. Contributor Grant.
Subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license

(a) under intellectual property rights (other than patent or trademark) Licensable by Contributor, to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code and/or as part of a Larger Work; and

(b) under Patent Claims infringed by the making, using, or selling of Modifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale, have made, and/or otherwise dispose of: 1) Modifications made by that Contributor (or portions thereof); and 2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination).

(c) the licenses granted in Sections 2.2(a) and 2.2(b) are effective on the date Contributor first makes Commercial Use of the Covered Code.

(d) Notwithstanding Section 2.2(b) above, no patent license is granted: 1) for any code that Contributor has deleted from the Contributor Version; 2) separate from the Contributor Version; 3) for infringements caused by: i) third party modifications of Contributor Version or ii) the combination of Modifications made by that Contributor with other software (except as part of the Contributor Version) or other devices; or 4) under Patent Claims infringed by Covered Code in the absence of Modifications made by that Contributor.

3. Distribution Obligations.

3.1. Application of License.
The Modifications which You create or to which You contribute are governed by the terms of this License, including without limitation Section 2.2. The Source Code version of Covered Code may be

distributed only under the terms of this License or a future version of this License released under Section 6.1, and You must include a copy of this License with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section 3.5.

3.2. Availability of Source Code.

Any Modification which You create or to which You contribute must be made available in Source Code form under the terms of this License either on the same media as an Executable version or via an accepted Electronic Distribution Mechanism to anyone to whom you made an Executable version available; and if made available via Electronic Distribution Mechanism, must remain available for at least twelve (12) months after the date it initially became available, or at least six (6) months after a subsequent version of that particular Modification has been made available to such recipients. You are responsible for ensuring that the Source Code version remains available even if the Electronic Distribution Mechanism is maintained by a third party.

3.3. Description of Modifications.

You must cause all Covered Code to which You contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

3.4. Intellectual Property Matters

(a) Third Party Claims.

If Contributor has knowledge that a license under a third party's intellectual property rights is required to exercise the rights granted by such Contributor under Sections 2.1 or 2.2, Contributor must include a text file with the Source Code distribution titled "LEGAL" which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If Contributor obtains such knowledge after the Modification is made available as described in Section 3.2, Contributor shall promptly modify the LEGAL file in all copies Contributor makes available thereafter and shall take other steps (such as notifying appropriate mailing lists or newsgroups) reasonably calculated to inform those who received the Covered

Code that new knowledge has been obtained.

(b) Contributor APIs.
If Contributor's Modifications include an application programming interface and Contributor has knowledge of patent licenses which are reasonably necessary to implement that API, Contributor must also include this information in the LEGAL file.

(c) Representations.
Contributor represents that, except as disclosed pursuant to Section 3.4(a) above, Contributor believes that Contributor's Modifications are Contributor's original creation(s) and/or Contributor has sufficient rights to grant the rights conveyed by

this License.

3.5. Required Notices.
You must duplicate the notice in Exhibit A in each file of the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If You created one or more Modification(s) You may add your name as a Contributor to the notice described in Exhibit A. You must also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Covered Code. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear than any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

3.6. Distribution of Executable Versions.
You may distribute Covered Code in Executable form only if the requirements of Section 3.1-3.5 have been met for that Covered Code, and if You include a notice stating that the Source Code version of the Covered Code is available under the terms of this License, including a description of how and where You have fulfilled the obligations of Section 3.2. The notice must be conspicuously included in any notice in an Executable version, related documentation or collateral in which You describe recipients' rights relating to the Covered Code. You may distribute the Executable
version of Covered
Code or ownership rights under a license of Your choice, which may

contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

3.7. Larger Works.
You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and
distribute the Larger
Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

4. Inability to Comply Due to Statute or Regulation.

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be included in the LEGAL file described in Section 3.4 and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Application of this License.

This License applies to code to which the Initial Developer has attached the notice in Exhibit A and to related Covered Code.

6. Versions of the License.

6.1. New Versions.
Netscape Communications Corporation ("Netscape") may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

6.2. Effect of New Versions.
Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms

of any subsequent version of the License published by Netscape. No one other than Netscape has the right to modify the terms applicable to Covered Code created under this License.

6.3. Derivative Works.

If You create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), You must (a) rename

Your license so that

the phrases "Mozilla", "MOZILLAPL", "MOZPL", "Netscape", "MPL", "NPL" or any confusingly similar phrase do not appear in your license (except to note that your license differs from this License) and (b) otherwise make it clear that Your version of the license contains terms which differ from the Mozilla Public License and Netscape Public License. (Filling in the name of the Initial Developer, Original Code or Contributor in the notice described in Exhibit A shall not of themselves be deemed to be modifications of this License.)

7. DISCLAIMER OF WARRANTY.

COVERED CODE IS PROVIDED UNDER THIS LICENSE ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE COVERED CODE IS FREE OF DEFECTS, MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE OR NON-INFRINGING. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE COVERED CODE IS WITH YOU. SHOULD ANY COVERED CODE PROVE DEFECTIVE IN ANY RESPECT, YOU (NOT THE INITIAL DEVELOPER OR ANY OTHER CONTRIBUTOR) ASSUME THE COST OF ANY NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED CODE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

8. TERMINATION.

8.1. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the Covered Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

8.2. If You initiate litigation by asserting a patent infringement claim (excluding declatory judgment actions) against Initial Developer or

a Contributor (the Initial Developer or Contributor against whom You file such action is referred to as "Participant") alleging that:

(a) such Participant's Contributor Version directly or indirectly infringes any patent, then any and all rights granted by such Participant to You under Sections 2.1 and/or 2.2 of this License shall, upon 60 days notice from Participant terminate prospectively, unless if within 60 days after receipt of notice You either: (i) agree in writing to pay Participant a mutually agreeable reasonable royalty for Your past and future use of Modifications made by such Participant, or (ii) withdraw Your litigation claim with respect to the Contributor Version against such Participant. If within 60 days of notice, a reasonable royalty and payment arrangement are not mutually agreed upon in writing by the parties or the litigation claim is not withdrawn, the rights granted by Participant to You under Sections 2.1 and/or 2.2 automatically terminate at the expiration of the 60 day notice period specified above.

(b) any software, hardware, or device, other than such Participant's Contributor Version, directly or indirectly infringes any patent, then any rights granted to You by such Participant under Sections 2.1(b) and 2.2(b) are revoked effective as of the date You first made, used, sold, distributed, or had made, Modifications made by that Participant.

8.3. If You assert a patent infringement claim against Participant alleging that such Participant's Contributor Version directly or indirectly infringes any patent where such claim is resolved (such as by license or settlement) prior to the initiation of patent infringement litigation, then the reasonable value of the licenses granted by such Participant under Sections 2.1 or 2.2 shall be taken into account in determining the amount or value of any payment or license.

8.4. In the event of termination under Sections 8.1 or 8.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or any distributor hereunder prior to termination shall survive termination.

9. LIMITATION OF LIABILITY.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU, THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF COVERED CODE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF

LIABILITY SHALL
NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY
RESULTING FROM SUCH PARTY'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW
PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE
EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO
THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

10. U.S. GOVERNMENT END USERS.

The Covered Code is a "commercial item," as that term is defined in
48 C.F.R. 2.101 (Oct. 1995), consisting of "commercial computer
software" and "commercial computer software documentation," as such
terms are used in 48 C.F.R. 12.212 (Sept. 1995). Consistent with 48
C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995),
all U.S. Government End Users acquire Covered Code with only those
rights set forth herein.

11. MISCELLANEOUS.

This License represents the complete agreement concerning subject
matter hereof. If any provision of this License is held to be
unenforceable,
such provision shall be reformed only to the extent
necessary to make it enforceable. This License shall be governed by
California law provisions (except to the extent applicable law, if
any, provides otherwise), excluding its conflict-of-law provisions.
With respect to disputes in which at least one party is a citizen of,
or an entity chartered or registered to do business in the United
States of America, any litigation relating to this License shall be
subject to the jurisdiction of the Federal Courts of the Northern
District of California, with venue lying in Santa Clara County,
California, with the losing party responsible for costs, including
without limitation, court costs and reasonable attorneys' fees and
expenses. The application of the United Nations Convention on
Contracts for the International Sale of Goods is expressly excluded.
Any law or regulation which provides that the language of a contract
shall be
construed against the drafter shall not apply to this
License.

12. RESPONSIBILITY FOR CLAIMS.

As between Initial Developer and the Contributors, each party is
responsible for claims and damages arising, directly or indirectly,
out of its utilization of rights under this License and You agree to
work with Initial Developer and Contributors to distribute such
responsibility on an equitable basis. Nothing herein is intended or
shall be deemed to constitute any admission of liability.

13. MULTIPLE-LICENSED CODE.

Initial Developer may designate portions of the Covered Code as "Multiple-Licensed". "Multiple-Licensed" means that the Initial Developer permits you to utilize portions of the Covered Code under Your choice of the NPL or the alternative licenses, if any, specified by the Initial Developer in the file described in Exhibit A.

EXHIBIT A -Mozilla Public License.

``The contents of this file are subject to the Mozilla Public License
Version 1.1 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.mozilla.org/MPL/

Software distributed under the License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License.

The Original Code is _____.

The Initial Developer of the Original Code is _____.
Portions created by _____ are Copyright (C) _____
_____. All Rights Reserved.

Contributor(s): _____.

Alternatively, the contents of this file may be used under the terms of the _____ license (the "[___] License"), in which case the provisions of [_____] License are applicable instead of those above. If
you wish to allow use of your version of this file only under the terms of the [____] License and not to allow others to use your version of this file under the MPL, indicate your decision by deleting the provisions above and replace them with the notice and other provisions required by the [___] License. If you do not delete the provisions above, a recipient may use your version of this file under either the MPL or the [___] License."

[NOTE: The text of this Exhibit A may differ slightly from the text of the notices in the Source Code files of the Original Code. You should use the text of this Exhibit A rather than the text found in the Original Code Source Code for Your Modifications.]

1.52 ethtool 4.6

1.52.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it. (Some other Free Software Foundation software is covered by
the GNU Lesser General Public License instead.)
You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price. Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid
anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate to certain responsibilities for you if you
distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether
gratis or for a fee, you must give the recipients
all the rights that
you have. You must make sure that they, too, receive or can get the
source code. And you must show them these terms so they know their
rights.

We protect your rights with two steps: (1) copyright the software, and
(2) offer you this license which gives you legal permission to copy,
distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain
that everyone understands that there is no warranty for this free
software. If the software is modified by someone else and passed on, we
want its recipients to know that what they have is not the original, so
that any problems introduced by others will not reflect on the original
authors' reputations.

Finally, any free program is threatened constantly by software
patents. We wish to avoid the danger
that redistributors of a free
program will individually obtain patent licenses, in effect making the
program proprietary. To prevent this, we have made it clear that any
patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and
modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains
a notice placed by the copyright holder saying it may be distributed
under the terms of this General Public License. The "Program", below,
refers to any such program or work, and a "work based on the Program"
means either the Program or any derivative work under copyright law:
that is to say, a work containing the Program or a portion
of it,
either verbatim or with modifications and/or translated into another
language. (Hereinafter, translation is included without limitation in
the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not
covered by this License; they are outside its scope. The act of
running the Program is not restricted, and the output from the Program
is covered only if its contents constitute a work based on the
Program (independent of having been made by running the Program).
Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's
source code as you receive it, in any medium, provided that you
conspicuously and appropriately publish on each copy an appropriate
copyright notice and disclaimer of warranty;
keep intact all the
notices that refer to this License and to the absence of any warranty;
and give any other recipients of the Program a copy of this License
along with the Program.

You may charge a fee for the physical act of transferring a copy, and

you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete

machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a

special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate
your rights under this License.
However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such

parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing

to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author

to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING,

REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option)
any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.
This
is free software, and you are welcome to redistribute it
under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than 'show w' and 'show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program 'Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General
Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

1.53 libsodium 1.0.1

1.53.1 Available under license :

```
/*
* ISC License
*
* Copyright (c) 2013-2019
* Frank Denis <j at pureftpd dot org>
*
* Permission to use, copy, modify, and/or distribute this software for any
* purpose with or without fee is hereby granted, provided that the above
* copyright notice and this permission notice appear in all copies.
*
* THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES
* WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF
* MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR
* ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
* WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
* ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF
* OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.
*/
```

1.54 libassuan 2.4.3

1.54.1 Available under license :

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts
as the successor of the GNU Library Public License, version 2, hence
the version number 2.1.]

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
Licenses are intended to guarantee your freedom to share and change
free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some
specially designated software packages--typically libraries--of the
Free Software Foundation and other authors who decide
to use it. You
can use it too, but we suggest you first think carefully about whether
this license or the ordinary General Public License is the better
strategy to use in any particular case, based on the explanations
below.

When we speak of free software, we are referring to freedom of use,
not price. Our General Public Licenses are designed to make sure that
you have the freedom to distribute copies of free software (and charge
for this service if you wish); that you receive source code or can get
it if you want it; that you can change the software and use pieces of
it in new free programs; and that you are informed that you can do
these things.

To protect your rights, we need to make restrictions that forbid
distributors to deny you these rights or to ask you to surrender these
rights. These restrictions translate to certain responsibilities for
you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether
gratis
or for a fee, you must give the recipients all the rights that we gave
you. You must make sure that they, too, receive or can get the source
code. If you link other code with the library, you must provide
complete object files to the recipients, so that they can relink them
with the library after making changes to the library and recompiling
it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the
library, and (2) we offer you this license, which gives you legal

permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the

free library to free
software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to
run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another
language. (Hereinafter, translation is
included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control

compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any

application-supplied function or table used by this function must
be optional: if the application does not supply it, the square
root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably
considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary
GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding

machine-readable source code, which
must be distributed under the terms of Sections 1 and 2 above on a
medium customarily used for software interchange.

If distribution of object code is made by offering access to copy
from a designated place, then offering equivalent access to copy the
source code from the same place satisfies the requirement to
distribute the source code, even though third parties are not
compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the
Library, but is designed to work with the Library by being compiled or
linked with it, is called a "work that uses the Library". Such a
work, in isolation, is not a derivative work of the Library, and
therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library
creates an executable that is a derivative of the Library (because it
contains portions of the Library), rather than a "work that uses
the
library". The executable is therefore covered by this License.
Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file
that is part of the Library, the object code for the work may be a
derivative work of the Library even though the source code is not.
Whether this is true is especially significant if the work can be
linked without the Library, or if the work is itself a library. The
threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data
structure layouts and accessors, and small macros and small inline
functions (ten lines or less in length), then the use of the object
file is unrestricted, regardless of whether it is legally a derivative
work. (Executables containing this object code plus portions of the
Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may
distribute the object
code for the work under the terms of Section 6.
Any executables containing that work also fall under Section 6,
whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or
link a "work that uses the Library" with the Library to produce a
work containing portions of the Library, and distribute that work
under terms of your choice, provided that the terms permit
modification of the work for the customer's own use and reverse

engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the
work with the complete corresponding
machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly
with a modified version of the library, if
the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is

normally
distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any
other library
facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you
do not accept this License. Therefore, by
modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the

Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse
you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system
which is
implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish
revised and/or new
versions of the Lesser General Public License from time to time.
Such new versions will be similar in spirit to the present version,
but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library
specifies a version number of this License which applies to it and
"any later version", you have the option of following the terms and
conditions either of that version or of any later version published by
the Free Software Foundation. If the Library does not specify a
license version number, you may choose any version ever published by
the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free
programs whose distribution conditions are incompatible with these,
write to the author to ask for permission. For software which is
copyrighted by the Free Software Foundation, write to the Free
Software Foundation; we sometimes make exceptions for this. Our
decision will
be guided by the two goals of preserving the free status
of all derivatives of our free software and of promoting the sharing
and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO
WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW.
EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR
OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY
KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE
LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME
THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN
WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY
AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE
LIABLE TO YOU
FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR
CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE
LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING
RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A
FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF
SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH
DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively
convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990

Ty Coon, President of Vice

That's all there is to it!

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for
software and other kinds of works.

The licenses for most software and other practical works are designed
to take away your freedom to share and change the works. By contrast,
the GNU General Public License is intended to guarantee your freedom to
share and change all versions of a program--to make sure it remains free
software for all its users. We, the Free Software Foundation, use the
GNU General Public License for most of our software; it applies also to
any other work released this way by its authors. You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price. Our General Public Licenses
are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
them if you wish), that you receive source code or can get it if you
want it, that you can change the software or use pieces of it in new
free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you
these rights or asking you to surrender the rights. Therefore, you have
certain responsibilities if you distribute copies of the software, or if
you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether
gratis or for a fee, you must pass on to the recipients the same
freedoms that you received. You must make sure that they, too, receive
or can get the source code. And you must show them these terms so they
know their rights.

Developers that use the GNU GPL protect your rights with two steps:
(1) assert copyright on the software, and (2) offer
you this License
giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains
in future versions
of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To
"modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate
Legal Notices"
to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than
the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all

the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users'

Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep
intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license
the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7

additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This

alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge.
You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object
code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute
modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because

modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you

add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections
15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional
terms are considered "further
restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may
not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your
receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time
you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not
impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control"
includes the right to grant
patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not

excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED,
INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer
of warranty and limitation of liability provided
above cannot be given local legal effect according to their terms,
reviewing courts shall apply local law that most closely approximates
an absolute waiver of all civil liability in connection with the
Program, unless a warranty or assumption of liability accompanies a
copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest
possible use to the public, the best way to achieve this is to make it
free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest
to attach them to the start of each source file to most effectively
state the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief

idea of what it does.>
  Copyright (C) <year> <name of author>

  This program is free software: you can redistribute it and/or modify
  it under the terms of the GNU General Public License as published by
  the Free Software Foundation, either version 3 of the License, or
  (at your option) any later version.

  This program is distributed in the hope that it will be useful,
  but WITHOUT ANY WARRANTY; without even the implied warranty of
  MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
  GNU General Public License for more details.

  You should have received a copy of the GNU General Public License
  along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

 If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

  <program> Copyright (C) <year> <name of author>
  This program comes with
 ABSOLUTELY NO WARRANTY; for details type `show w'.
  This is free software, and you are welcome to redistribute it
  under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

 You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

 The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what you want to do, use the GNU Lesser General
Public License instead of this License. But first,
 please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.

1.55 grep 2.25

1.55.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <https://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for
software and other kinds of works.

The licenses for most software and other practical works are designed
to take away your freedom to share and change the works. By contrast,
the GNU General Public License is intended to guarantee your freedom to
share and change all versions of a program--to make sure it remains free
software for all its users. We, the Free Software Foundation, use the
GNU General Public License for most of our software; it applies also to
any other work released this way by its authors. You can apply it to
your programs, too.

When we speak of free software, we are referring to
freedom, not
price. Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
them if you wish), that you receive source code or can get it if you
want it, that you can change the software or use pieces of it in new
free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you
these rights or asking you to surrender the rights. Therefore, you have
certain responsibilities if you distribute copies of the software, or if
you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether
gratis or for a fee, you must pass on to the recipients the same
freedoms that you received. You must make sure that they, too, receive
or can get the source code. And you must show them these terms so they
know their rights.

Developers that use the GNU GPL protect your rights with two steps:
(1)
assert copyright on the software, and (2) offer you this License
giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains
that there is no warranty for this free software. For both users' and

authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand
ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees"
and
"recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy,
is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The
"System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's

System Libraries, or general-purpose tools or generally
available free
programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is
covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed;
section 10
makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article

11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately
publish on each copy an appropriate copyright notice;
keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated
place (gratis or for a charge), and offer equivalent access to the
Corresponding Source in
the same way through the same place at no
further charge. You need not require recipients to copy the
Corresponding Source along with the object code. If the place to
copy the object code is a network server, the Corresponding Source
may be on a different server (operated by you or a third party)
that supports equivalent copying facilities, provided you maintain
clear directions next to the object code saying where to find the
Corresponding Source. Regardless of what server hosts the
Corresponding Source, you remain obligated to ensure that it is
available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided
you inform other peers where the object code and Corresponding
Source of the work are being offered to the general public at no
charge under subsection 6d.

A separable portion of the object code, whose source code is excluded
from the Corresponding Source
as a System Library, need not be
included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any
tangible personal property which is normally used for personal, family,
or household purposes, or (2) anything designed or sold for incorporation
into a dwelling. In determining whether a product is a consumer product,
doubtful cases shall be resolved in favor of coverage. For a particular
product received by a particular user, "normally used" refers to a
typical or common use of that class of product, regardless of the status
of the particular user or of the way in which the particular user
actually uses, or expects or is expected to use, the product. A product
is a consumer product regardless of whether the product has substantial
commercial, industrial or non-consumer uses, unless such uses represent
the only significant mode of use of the product.

"Installation Information" for a User Product means any methods,
procedures, authorization
keys, or other information required to install
and execute modified versions of a covered work in that User Product from
a modified version of its Corresponding Source. The information must
suffice to ensure that the continued functioning of the modified object
code is in no case prevented or interfered with solely because
modification has been made.

If you convey an object code work under this section in, or with, or
specifically for use in, a User Product, and the conveying occurs as

part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in
ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the
entire Program shall
be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty

or limiting liability differently from the
terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or
author attributions in that material or in the Appropriate Legal
Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or
requiring that modified versions of such material be marked in
reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or
authors of the material; or

e) Declining to grant rights under trademark law for use of some
trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that
material by anyone who conveys the material (or modified versions of
it) with contractual assumptions of liability to the recipient, for
any liability that these contractual assumptions directly impose on

those licensors and authors.

All other non-permissive additional terms are considered "further
restrictions" within the meaning of section 10. If the Program as you
received it, or any part of it, contains a notice stating that it is
governed by this License along with a term that is a further
restriction, you may remove that term. If a license document contains
a further restriction but permits relicensing or conveying under this
License, you may add to a covered work material governed by the terms
of that license document, provided that the further restriction does
not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you
must place, in the relevant source files, a statement of the
additional terms that apply to those files, or a notice indicating
where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the
form of a separately written license, or stated as exceptions;
the above
requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly
provided under this License. Any attempt otherwise to propagate or

modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright
holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever

licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights
granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For
purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this
License, through a
publicly available network server or other readily accessible means,

then you must either (1) cause the Corresponding Source to be so
available, or (2) arrange to deprive yourself of the benefit of the
patent license for this particular work, or (3) arrange, in a manner
consistent with the requirements of this License, to extend the patent
license to downstream recipients. "Knowingly relying" means you have
actual knowledge that, but for the patent license, your conveying the
covered work in a country, or your recipient's use of the covered work
in a country, would infringe one or more identifiable patents in that
country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or
arrangement, you convey, or propagate by procuring conveyance of, a
covered work, and grant a patent license to some of the parties
receiving the covered work authorizing them to use, propagate, modify
or convey a specific copy of the covered
work, then the patent license
you grant is automatically extended to all recipients of the covered
work and works based on it.

A patent license is "discriminatory" if it does not include within
the scope of its coverage, prohibits the exercise of, or is
conditioned on the non-exercise of one or more of the rights that are
specifically granted under this License. You may not convey a covered
work if you are a party to an arrangement with a third party that is
in the business of distributing software, under which you make payment
to the third party based on the extent of your activity of conveying
the work, and under which the third party grants, to any of the
parties who would receive the covered work from you, a discriminatory
patent license (a) in connection with copies of the covered work
conveyed by you (or copies made from those copies), or (b) primarily
for and in connection with specific products or compilations that
contain the covered work, unless you entered into that arrangement,
or
that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting
any implied license or other defenses to infringement that may
otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or
otherwise) that contradict the conditions of this License, they do not
excuse you from the conditions of this License. If you cannot convey a
covered work so as to satisfy simultaneously your obligations under this
License and any other pertinent obligations, then as a consequence you may
not convey it at all. For example, if you agree to terms that obligate you
to collect a royalty for further conveying from those to whom you convey

the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS"

WITHOUT WARRANTY
OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17.
Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by

the Free Software Foundation, either version 3 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program. If not, see <https://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>
This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<https://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what you want
to do, use the GNU Lesser General
Public License instead of this License. But first, please read
<https://www.gnu.org/licenses/why-not-lgpl.html>.

1.56 lxc 2.0.4

1.56.1 Available under license :

The MIT License (MIT)

Copyright (c) 2015 Ryan Faerman

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal

in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all
copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR
IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
SOFTWARE.
Extensions of the original work are copyright (c) 2011 Miek Gieben

As this is fork of the official Go code the same license applies:

Copyright (c) 2009 The Go Authors. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are
met:

* Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above
copyright notice, this list of conditions and the following disclaimer
in the documentation and/or other materials provided with the
distribution.
* Neither the name of Google Inc. nor the names of its
contributors may be used to endorse or promote products derived from
this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED
TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT
OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

```
// Copyright  2015 Steve Francia <spf@spf13.com>.
//
// Licensed under the Apache License, Version 2.0 (the "License");
// you may not use this file except in compliance with the License.
// You may obtain a copy of the License at
// http://www.apache.org/licenses/LICENSE-2.0
//
// Unless required by applicable law or agreed to in writing, software
// distributed under the License is distributed on an "AS IS" BASIS,
// WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
// See the License for the specific language governing permissions and
// limitations under the License.

// Parts inspired by https://github.com/ryanuber/go-license

package cmd

func initGpl2() {
 Licenses["gpl2"] = License{
  Name:            "GNU General Public License 2.0",
  PossibleMatches: []string{"gpl2", "gnu gpl2", "gplv2"},
  Header: `
This program is free software; you can redistribute it and/or
modify it under the terms of the GNU General Public License
as published by the Free Software
 Foundation; either version 2
of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
GNU General Public License for more details.

You should have received a copy of the GNU Lesser General Public License
along with this program. If not, see <http://www.gnu.org/licenses/>.`,
  Text: `                GNU GENERAL PUBLIC LICENSE
                Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

                        Preamble

 The licenses for most software are designed to take away your
freedom to share and change it.  By contrast, the GNU General Public
License is intended to
```

guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it. (Some other Free Software Foundation software is covered by
the GNU Lesser General Public License instead.) You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price. Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid
anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate to certain
responsibilities for you if you
distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether
gratis or for a fee, you must give the recipients all the rights that
you have. You must make sure that they, too, receive or can get the
source code. And you must show them these terms so they know their
rights.

We protect your rights with two steps: (1) copyright the software, and
(2) offer you this license which gives you legal permission to copy,
distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain
that everyone understands that there is no warranty for this free
software. If the software is modified by someone else and passed on, we
want its recipients to know that what they have is not the original, so
that any problems introduced by others will not reflect on the original
authors' reputations.

Finally, any free program is threatened constantly by software
patents.
We wish to avoid the danger that redistributors of a free
program will individually obtain patent licenses, in effect making the
program proprietary. To prevent this, we have made it clear that any
patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and
modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such

interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there
is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus,
it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third
party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer

to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed
need not include
anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in
full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following
notices to the program. It is safest
to attach them to the start of each source file to most effectively
convey the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation; either version 2 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License along
with this program; if not, write to the Free
Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than 'show w' and 'show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter
the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
'Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this is what you want to do, use the GNU Lesser General
Public License instead of this License.
`,
 }
}
Copyright 2013, Roger Peppe
All rights reserved.

Redistribution and use in source and binary forms, with or without modification,
are permitted provided that the following conditions are met:

  * Redistributions of source code must retain the above copyright notice,
    this list of conditions and the following disclaimer.
  * Redistributions in binary form must reproduce the above copyright notice,
    this list of conditions and the following disclaimer in the documentation
    and/or other materials provided with the distribution.
  * Neither the name of this project nor the names of its contributors
    may be used to endorse or promote products derived from this software
    without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT
 SHALL THE COPYRIGHT
OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED
TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR
PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
Copyright (c) 2012 Alex Ogier. All rights reserved.
Copyright (c) 2012 The Go Authors. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are
met:

  * Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
  * Redistributions in binary form must reproduce the above

copyright notice, this list of conditions and the following disclaimer
in the documentation and/or other materials provided with the
distribution.
  * Neither the name of Google Inc. nor the names of its
contributors may be used to endorse or promote products derived from
this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR PURPOSE
 ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT
OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
Copyright (C) 2011-2015 Canonical Ltd.
This software is licensed under the LGPLv3, included below.

As a special exception to the GNU Lesser General Public License version 3
("LGPL3"), the copyright holders of this Library give you permission to
convey to a third party a Combined Work that links statically or dynamically
to this Library without providing any Minimal Corresponding Source or
Minimal Application Code as set out in 4d or providing the installation
information set out in section 4e, provided that you comply with the other
provisions of LGPL3 and provided that you meet, for the Application the
terms and conditions of the license(s) which apply to the Application.

Except as stated in this special exception, the provisions of LGPL3 will
continue to comply in full to this Library. If you modify this Library, you
may apply this exception to your version of this Library, but you are not
obliged to do so. If you do not wish to do so, delete this exception
statement from your version.
 This exception does not (and cannot) modify any
license terms which apply to the Application, with which you must still
comply.

GNU LESSER GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and the "GNU GPL" refers to version 3 of the GNU General Public License.

"The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An "Application" is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions
of the GNU Lesser General Public License from time to time. Such new
versions will be similar in spirit to the present version, but may
differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the
Library as you received it specifies
that a certain numbered version
of the GNU Lesser General Public License "or any later version"
applies to it, you have the option of following the terms and
conditions either of that published version or of any later version
published by the Free Software Foundation. If the Library as you
received it does not specify a version number of the GNU Lesser
General Public License, you may choose any version of the GNU Lesser
General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide
whether future versions of the GNU Lesser General Public License shall
apply, that proxy's public statement of acceptance of any version is
permanent authorization for you to choose that version for the
Library.
/*
Copyright 2014 The Go4 Authors

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

    http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
*/

// Package legal provides in-process storage for compiled-in licenses.
package legal

var licenses []string

// RegisterLicense stores the license text.
// It doesn't check whether the text was already present.
func RegisterLicense(text string) {
 licenses = append(licenses, text)
 return
}

```
// Licenses returns a slice of the licenses.
func Licenses() []string {
 return licenses
}
```

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial

revisions, annotations, elaborations, or other modifications
represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License,
each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute
copies of the
Work or Derivative Works thereof in any medium, with or without
modifications, and in Source or Object form, provided that You
meet the following conditions:

(a) You must give any other recipients of the Work or
Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices
stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works
that You distribute, all copyright, patent, trademark, and
attribution notices from the Source form of the Work,
excluding those notices that do not pertain to any part of
the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its
distribution, then any Derivative Works that You distribute must
include a readable copy of the attribution notices contained
within such NOTICE file, excluding
those notices that do not
pertain to any part of the Derivative Works, in at least one
of the following places: within a NOTICE text file distributed
as part of the Derivative Works; within the Source form or
documentation, if provided along with the Derivative Works; or,
within a display generated by the Derivative Works, if and
wherever such third-party notices normally appear. The contents
of the NOTICE file are for informational purposes only and
do not modify the License. You may add Your own attribution
notices within Derivative Works that You distribute, alongside
or as an addendum to the NOTICE text from the Work, provided
that such additional attribution notices cannot be construed
as modifying the License.

You may add Your own copyright statement to Your modifications and
may provide additional or different license terms and conditions

for use, reproduction, or distribution of Your modifications, or
for any such Derivative Works as a whole, provided Your use,
reproduction, and distribution of the Work otherwise complies with
the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise,
any Contribution intentionally submitted for inclusion in the Work
by You to the Licensor shall be under the terms and conditions of
this License, without any additional terms or conditions.

Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.

The MIT License (MIT)

Copyright (c) 2014 Yasuhiro Matsumoto

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all
copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT
OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Copyright (c) 2015, Dave Cheney <dave@cheney.net>
All rights reserved.

Redistribution and use in source and binary forms, with or without

modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this
 list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice,
 this list of conditions and the following disclaimer in the documentation
 and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE
 GOODS OR
SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER
CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,
OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
Copyright (c) 2012, 2013 Ugorji Nwoke.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification,
are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice,
 this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright notice,
 this list of conditions and the following disclaimer in the documentation
 and/or other materials provided with the distribution.
* Neither the name of the author nor the names of its contributors may be used
 to endorse or promote products derived from this software
 without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT
 HOLDER OR CONTRIBUTORS BE LIABLE FOR
ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES
(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON
ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
Format: http://www.debian.org/doc/packaging-manuals/copyright-format/1.0/
Upstream-Name: golang-petname

Upstream-Contact: Dustin Kirkland <dustin.kirkland@gmail.com>
Source: http://launchpad.net/golang-petname

Files: *
Copyright: 2014, Dustin Kirkland <dustin.kirkland@gmail.com>
License: Apache-2
Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at
http://www.apache.org/licenses/LICENSE-2.0
Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
On Debian systems, the complete text of the Apache version 2.0 license
can be found in "/usr/share/common-licenses/Apache-2.0".
Copyright (c) 2013 The Gorilla WebSocket Authors. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this
list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice,
this list of conditions and the following disclaimer in the documentation
and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE
GOODS OR
SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER
CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,
OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
The author disclaims copyright to this source code. In place of
a legal notice, here is a blessing:

May you do good and not evil.
May you find forgiveness for yourself and forgive others.
May you share freely, never taking more than you give.
Copyright 2011-2016 Canonical Ltd.

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
Copyright (c) 2013 Julien Schmidt. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright
  notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.
* The names of the contributors may not be used to endorse or promote
  products derived from this software without specific prior written
  permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
DISCLAIMED. IN NO EVENT SHALL JULIEN SCHMIDT BE
LIABLE FOR ANY
DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES
(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND
ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
Copyright 2014 Alan Shreve

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and

limitations under the License.
Copyright 2013 Suryandaru Triandana <syndtr@gmail.com>
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are
met:

  * Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
  * Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT
HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
LIMITED TO, PROCUREMENT OF SUBSTITUTE
 GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
All files in this repository are licensed as follows. If you contribute
to this repository, it is assumed that you license your contribution
under the same license unless you state otherwise.

All files Copyright (C) 2015 Canonical Ltd. unless otherwise specified in the file.

This software is licensed under the LGPLv3, included below.

As a special exception to the GNU Lesser General Public License version 3
("LGPL3"), the copyright holders of this Library give you permission to
convey to a third party a Combined Work that links statically or dynamically
to this Library without providing any Minimal Corresponding Source or
Minimal Application Code as set out in 4d or providing the installation
information set out in section 4e, provided that you comply with the other
provisions of LGPL3 and provided that you meet, for the Application the
terms and conditions of the license(s) which apply to the Application.

Except as stated in this special exception, the provisions of LGPL3 will
continue
 to comply in full to this Library. If you modify this Library, you
may apply this exception to your version of this Library, but you are not
obliged to do so. If you do not wish to do so, delete this exception

statement from your version. This exception does not (and cannot) modify any license terms which apply to the Application, with which you must still comply.

GNU LESSER GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and the
"GNU GPL" refers to version 3 of the GNU
General Public License.

"The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An "Application" is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The "Corresponding Application Code" for a Combined Work means the object
code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

a) Give prominent notice with each copy of the Combined Work that

the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

Copyright 2014, Roger Peppe, Canonical Inc.

This software is licensed under the LGPLv3, included below.

As a special exception to the GNU Lesser General Public License version 3 ("LGPL3"), the copyright holders of this Library give you permission to convey to a third party a Combined Work that links statically or dynamically to this Library without providing any Minimal Corresponding Source or Minimal Application Code as set out in 4d or providing the installation information set out in section 4e, provided that you comply with the other provisions of LGPL3 and provided that you meet, for the Application the terms and conditions of the license(s) which apply to the Application.

Except as stated in this special exception, the provisions of LGPL3 will continue to comply in full to this Library. If you modify this Library, you

may apply this exception to your version of this Library, but you are not obliged to do so. If you do not wish to do so, delete this exception statement from your
version. This exception does not (and cannot) modify any license terms which apply to the Application, with which you must still comply.

GNU LESSER GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and the "GNU GPL" refers to version 3 of the GNU General Public License.

"The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An "Application" is any work that
makes use of an interface provided
by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the

Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section
3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License
without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a
facility refers to a function or data to be supplied by an Application
that uses the facility (other than as an argument passed when the
facility is invoked), then you may convey a copy of the modified
version:

a) under this License, provided that you make a good faith effort to
ensure that, in the event an Application does not supply the
function or data, the facility still operates, and performs
whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of
this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from
a header file that is part of the Library.
You may convey such object
code under terms of your choice, provided that, if the incorporated
material is not limited to numerical parameters, data structure
layouts and accessors, or small macros, inline functions and templates
(ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the
Library is used in it and that the Library and its use are
covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license
document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that,
taken together, effectively do not restrict modification of the
portions of the Library contained in the Combined Work and reverse
engineering for debugging such modifications, if you also do each of
the following:

a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a

single library together with other library
facilities that are not Applications and are not covered by this
License, and convey such a combined library under terms of your
choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based
on the Library, uncombined with any other library facilities,
conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it
is a work based on the Library, and explaining where to find the
accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions
of the GNU Lesser General Public License from time to time. Such new
versions will be similar in spirit to the present version, but may
differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the
Library as you received
it specifies that a certain numbered version
of the GNU Lesser General Public License "or any later version"
applies to it, you have the option of following the terms and
conditions either of that published version or of any later version
published by the Free Software Foundation. If the Library as you
received it does not specify a version number of the GNU Lesser
General Public License, you may choose any version of the GNU Lesser
General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide
whether future versions of the GNU Lesser General Public License shall
apply, that proxy's public statement of acceptance of any version is
permanent authorization for you to choose that version for the
Library.
Mozilla Public License, version 2.0

1. Definitions

1.1. Contributor

means each individual or legal entity that creates, contributes to the
creation of, or owns Covered Software.

1.2. Contributor Version

means the combination of the Contributions of others (if any) used by a

Contributor and that particular Contributors Contribution.

1.3. Contribution

means Covered Software of a particular Contributor.

1.4. Covered Software

means Source Code Form to which the initial Contributor has attached the notice in Exhibit A, the Executable Form of such Source Code Form, and Modifications of such Source Code Form, in each case including portions thereof.

1.5. Incompatible With Secondary Licenses
means

a. that the initial Contributor has attached the notice described in Exhibit B to the Covered Software; or

b. that the Covered Software was made available under the terms of version 1.1 or earlier of the License, but
not also under the terms of a
Secondary License.

1.6. Executable Form

means any form of the work other than Source Code Form.

1.7. Larger Work

means a work that combines Covered Software with other material, in a separate file or files, that is not Covered Software.

1.8. License

means this document.

1.9. Licensable

means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently, any and all of the rights conveyed by this License.

1.10. Modifications

means any of the following:

a. any file in Source Code Form that results from an addition to, deletion

from, or modification of the contents of Covered Software; or

b. any new file in Source Code Form that contains any Covered Software.

1.11. Patent Claims of a Contributor

means any patent claim(s), including without limitation, method, process, and apparatus claims, in any patent Licensable by such Contributor that would be infringed, but for the grant of the License, by the making, using, selling, offering for sale, having made, import, or transfer of either its Contributions or its Contributor Version.

1.12. Secondary License

means either the GNU General Public License, Version 2.0, the GNU Lesser General Public License, Version 2.1, the GNU Affero General Public License, Version 3.0, or any later versions of those licenses.

1.13. Source Code Form

means the form of the work preferred for making modifications.

1.14. You (or Your)

means an individual or a legal entity exercising rights under this License. For legal entities, You includes any entity that controls, is controlled by, or is under common control with You. For purposes of this definition, control means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. License Grants and Conditions

2.1. Grants

Each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license:

a. under intellectual property rights (other than patent or trademark) Licensable by such Contributor to use, reproduce, make available, modify, display, perform, distribute, and otherwise exploit its Contributions, either on an unmodified basis, with Modifications, or as part of a Larger Work; and

b. under Patent Claims of such Contributor to make, use, sell, offer for sale, have made, import, and otherwise transfer either its Contributions or its Contributor Version.

2.2. Effective Date

The licenses granted in Section 2.1 with respect to any Contribution become effective for each Contribution on the date the Contributor first distributes such Contribution.

2.3.
Limitations on Grant Scope

The licenses granted in this Section 2 are the only rights granted under this License. No additional rights or licenses will be implied from the distribution or licensing of Covered Software under this License. Notwithstanding Section 2.1(b) above, no patent license is granted by a Contributor:

a. for any code that a Contributor has removed from Covered Software; or

b. for infringements caused by: (i) Your and any other third partys modifications of Covered Software, or (ii) the combination of its Contributions with other software (except as part of its Contributor Version); or

c. under Patent Claims infringed by Covered Software in the absence of its Contributions.

This License does not grant any rights in the trademarks, service marks, or logos of any Contributor (except as may be necessary to comply with the notice requirements in Section 3.4).

2.4. Subsequent
Licenses

No Contributor makes additional grants as a result of Your choice to distribute the Covered Software under a subsequent version of this License (see Section 10.2) or under the terms of a Secondary License (if permitted under the terms of Section 3.3).

2.5. Representation

Each Contributor represents that the Contributor believes its Contributions are its original creation(s) or it has sufficient rights to grant the rights to its Contributions conveyed by this License.

2.6. Fair Use

This License is not intended to limit any rights You have under applicable copyright doctrines of fair use, fair dealing, or other equivalents.

2.7. Conditions

Sections 3.1, 3.2, 3.3, and 3.4 are conditions of the licenses granted in Section 2.1.

3. Responsibilities

3.1. Distribution of Source Form

All distribution of Covered Software in Source Code Form, including any Modifications that You create or to which You contribute, must be under the terms of this License. You must inform recipients that the Source Code Form of the Covered Software is governed by the terms of this License, and how they can obtain a copy of this License. You may not attempt to alter or restrict the recipients rights in the Source Code Form.

3.2. Distribution of Executable Form

If You distribute Covered Software in Executable Form then:

a. such Covered Software must also be made available in Source Code Form, as described in Section 3.1, and You must inform recipients of the Executable Form how they can obtain a copy of such Source Code Form by reasonable means in a timely manner, at a charge no more than the cost of distribution to the recipient; and

b. You may distribute such Executable Form under the terms of this License, or sublicense it under different terms, provided that the license for the Executable Form does not attempt to limit or alter the recipients rights in the Source Code Form under this License.

3.3. Distribution of a Larger Work

You may create and distribute a Larger Work under terms of Your choice, provided that You also comply with the requirements of this License for the Covered Software. If the Larger Work is a combination of Covered Software with a work governed by one or more Secondary Licenses, and the Covered Software is not Incompatible With Secondary Licenses, this License permits You to additionally distribute such Covered Software under the terms of such Secondary License(s), so that the recipient of the Larger Work may, at their option, further distribute the Covered Software under the terms of either this License or such Secondary License(s).

3.4. Notices

You may not remove or alter the substance of any license notices (including copyright notices, patent notices, disclaimers of warranty, or limitations of liability) contained within the Source Code Form of the Covered Software, except that You may alter any license notices to the extent required to remedy known factual inaccuracies.

3.5. Application of Additional Terms

You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Software. However, You may do so only on Your own behalf, and not on behalf of any Contributor. You must make it absolutely clear that any such warranty, support, indemnity, or liability obligation is offered by You alone, and You hereby agree to indemnify every Contributor for any liability incurred by such Contributor as a result of warranty, support, indemnity or liability terms You offer. You may include additional disclaimers of warranty and limitations of liability specific to any jurisdiction.

4. Inability to Comply Due to Statute or Regulation

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Software due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be placed in a text file included with all distributions of the Covered Software under this License. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Termination

5.1. The rights granted under this License will terminate automatically if You fail to comply with any of its terms. However, if You become compliant, then the rights granted under this License from a particular Contributor are reinstated (a) provisionally, unless and until such Contributor explicitly and finally terminates Your grants, and (b) on an ongoing basis, if such Contributor fails to notify You of the non-compliance by some reasonable means prior to 60 days after You have come back into compliance. Moreover, Your grants from a particular Contributor are reinstated on an ongoing basis if such Contributor notifies You of the non-compliance by

some reasonable means, this is the first time You have received notice of non-compliance with this License from such Contributor, and You become compliant prior to 30 days after Your receipt of the notice.

5.2. If You initiate litigation against any entity by asserting a patent infringement claim (excluding declaratory judgment actions, counter-claims, and cross-claims) alleging that a Contributor Version directly or indirectly infringes any patent, then the rights granted to You by any and all Contributors for the Covered Software under Section 2.1 of this License shall terminate.

5.3. In the event of termination under Sections 5.1 or 5.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or Your distributors under this License prior to termination shall survive termination.

6. Disclaimer of Warranty

Covered Software is provided under this License on an as is basis, without warranty of any kind, either expressed, implied, or statutory, including, without limitation, warranties that the Covered Software is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the Covered Software is with You. Should any Covered Software prove defective in any respect, You (not any Contributor) assume the cost of any necessary servicing, repair, or correction. This disclaimer of warranty constitutes an essential part of this License. No use of any Covered Software is authorized under this License except under this disclaimer.

7. Limitation of Liability

Under no circumstances and under no legal theory, whether tort (including negligence), contract, or otherwise, shall any Contributor, or anyone who distributes Covered Software as permitted above, be liable to You for any direct, indirect, special, incidental, or consequential damages of any character including, without limitation, damages for lost profits, loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses, even if such party shall have been informed of the possibility of such damages. This limitation of liability shall not apply to liability for death or personal injury resulting from such partys negligence to the extent applicable law prohibits such limitation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this exclusion and limitation may not apply to You.

8. Litigation

Any litigation relating to this License
may be brought only in the courts of
a jurisdiction where the defendant maintains its principal place of business
and such litigation shall be governed by laws of that jurisdiction, without
reference to its conflict-of-law provisions. Nothing in this Section shall
prevent a partys ability to bring cross-claims or counter-claims.

9. Miscellaneous

This License represents the complete agreement concerning the subject matter
hereof. If any provision of this License is held to be unenforceable, such
provision shall be reformed only to the extent necessary to make it
enforceable. Any law or regulation which provides that the language of a
contract shall be construed against the drafter shall not be used to construe
this License against a Contributor.

10. Versions of the License

10.1. New Versions

Mozilla Foundation is the license steward. Except as provided in Section
10.3, no one other than the license steward has the right to modify or
publish new versions of this License. Each version will be given a
distinguishing version number.

10.2. Effect of New Versions

You may distribute the Covered Software under the terms of the version of
the License under which You originally received the Covered Software, or
under the terms of any subsequent version published by the license
steward.

10.3. Modified Versions

If you create software not governed by this License, and you want to
create a new license for such software, you may create and use a modified
version of this License if you rename the license and remove any
references to the name of the license steward (except to note that such
modified license differs from this License).

10.4. Distributing Source Code Form that is Incompatible With Secondary Licenses
If You choose to distribute Source Code Form that is Incompatible With
Secondary Licenses under the terms of this version of the License,
the
notice described in Exhibit B of this License must be attached.

Exhibit A - Source Code Form License Notice

This Source Code Form is subject to the
terms of the Mozilla Public License, v.
2.0. If a copy of the MPL was not
distributed with this file, You can
obtain one at
http://mozilla.org/MPL/2.0/.

If it is not possible or desirable to put the notice in a particular file, then
You may include the notice in a location (such as a LICENSE file in a relevant
directory) where a recipient would be likely to look for such a notice.

You may add additional accurate notices of copyright ownership.

Exhibit B - Incompatible With Secondary Licenses Notice

This Source Code Form is Incompatible
With Secondary Licenses, as defined by
the Mozilla Public License, v. 2.0.

Copyright (c) 2013, Patrick Mezard
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are
met:

Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.
The names of its contributors may not be used to endorse or promote
products derived from this software without specific prior written
permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS
IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT
HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY
DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED
TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR
PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Mozilla Public License, version 2.0

1. Definitions

1.1. "Contributor"

means each individual or legal entity that creates, contributes to the creation of, or owns Covered Software.

1.2. "Contributor Version"

means the combination of the Contributions of others (if any) used by a Contributor and that particular Contributor's Contribution.

1.3. "Contribution"

means Covered Software of a particular Contributor.

1.4. "Covered Software"

means Source Code Form to which the initial Contributor has attached the notice in Exhibit A, the Executable Form of such Source Code Form, and Modifications of such Source Code Form, in each case including portions thereof.

1.5. "Incompatible With Secondary Licenses"
means

a. that the initial Contributor has attached the notice described in Exhibit B to the Covered Software; or

b. that the Covered Software was made available under the terms of version 1.1 or earlier of the
License, but not also under the terms of
a Secondary License.

1.6. "Executable Form"

means any form of the work other than Source Code Form.

1.7. "Larger Work"

means a work that combines Covered Software with other material, in a separate file or files, that is not Covered Software.

1.8. "License"

means this document.

1.9. "Licensable"

means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently, any and all of the rights conveyed by this License.

1.10. "Modifications"

means any of the following:

a. any file in Source Code Form that results from an addition to, deletion from, or modification of the contents of Covered Software; or

b. any new file in Source Code Form that contains any Covered Software.

1.11. "Patent Claims" of a Contributor

means any patent claim(s), including without limitation, method, process, and apparatus claims, in any patent Licensable by such Contributor that would be infringed, but for the grant of the License, by the making, using, selling, offering for sale, having made, import, or transfer of either its Contributions or its Contributor Version.

1.12. "Secondary License"

means either the GNU General Public License, Version 2.0, the GNU Lesser General Public License, Version 2.1, the GNU Affero General Public License, Version 3.0, or any later versions of those licenses.

1.13. "Source Code Form"

means the form of the work preferred for making modifications.

1.14. "You" (or "Your")

means an individual or a legal entity exercising rights under this License. For legal entities, "You" includes any entity that controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. License Grants and Conditions

2.1. Grants

Each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license:

a. under intellectual property rights (other than patent or trademark) Licensable by such Contributor to use, reproduce, make available, modify, display, perform, distribute, and otherwise exploit its Contributions, either on an unmodified basis, with Modifications, or as part of a Larger Work; and

b. under Patent Claims of such Contributor to make, use, sell, offer for sale, have made, import, and otherwise transfer either its Contributions or its Contributor Version.

2.2. Effective Date

The licenses granted in Section 2.1 with respect to any Contribution become effective for each Contribution on the date the Contributor first distributes such Contribution.

2.3. Limitations on Grant Scope

The licenses granted in this Section 2 are the only rights granted under this License. No additional rights or licenses will be implied from the distribution or licensing of Covered Software under this License. Notwithstanding Section 2.1(b) above, no patent license is granted by a Contributor:

a. for any code that a Contributor has removed from Covered Software; or

b. for infringements caused by: (i) Your and any other third party's modifications of Covered Software, or (ii) the combination of its Contributions with other software (except as part of its Contributor Version); or

c. under Patent Claims infringed by Covered Software in the absence of its Contributions.

This License does not grant any rights in the trademarks, service marks, or logos of any Contributor (except as may be necessary to comply with the notice requirements in Section 3.4).

2.4. Subsequent Licenses

No Contributor makes additional grants as a result of Your choice to distribute the Covered Software under a subsequent version of this License (see Section 10.2) or under the terms of a Secondary License (if permitted under the terms of Section 3.3).

2.5. Representation

Each Contributor represents that the Contributor believes its Contributions are its original creation(s) or it has sufficient rights to grant the rights to its Contributions conveyed by this License.

2.6. Fair Use

This License is not intended to limit any rights You have under applicable copyright doctrines of fair use, fair dealing, or other equivalents.

2.7. Conditions

Sections 3.1, 3.2, 3.3, and 3.4 are conditions of the licenses granted in Section 2.1.

3. Responsibilities

3.1. Distribution of Source Form

All distribution of Covered Software in Source Code Form, including any Modifications
that You create or to which You contribute, must be under the terms of this License. You must inform recipients that the Source Code Form of the Covered Software is governed by the terms of this License, and how they can obtain a copy of this License. You may not attempt to alter or restrict the recipients' rights in the Source Code Form.

3.2. Distribution of Executable Form

If You distribute Covered Software in Executable Form then:

a. such Covered Software must also be made available in Source Code Form, as described in Section 3.1, and You must inform recipients of the Executable Form how they can obtain a copy of such Source Code Form by reasonable means in a timely manner, at a charge no more than the cost of distribution to the recipient; and

b. You may distribute such Executable Form under the terms of this License, or sublicense it under different terms, provided that the

license
for the Executable Form does not attempt to limit or alter the
recipients' rights in the Source Code Form under this License.

3.3. Distribution of a Larger Work

You may create and distribute a Larger Work under terms of Your choice, provided that You also comply with the requirements of this License for the Covered Software. If the Larger Work is a combination of Covered Software with a work governed by one or more Secondary Licenses, and the Covered Software is not Incompatible With Secondary Licenses, this License permits You to additionally distribute such Covered Software under the terms of such Secondary License(s), so that the recipient of the Larger Work may, at their option, further distribute the Covered Software under the terms of either this License or such Secondary License(s).

3.4. Notices

You may not remove or alter the substance of any license notices (including copyright notices, patent notices, disclaimers
of warranty, or
limitations of liability) contained within the Source Code Form of the Covered Software, except that You may alter any license notices to the extent required to remedy known factual inaccuracies.

3.5. Application of Additional Terms

You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Software. However, You may do so only on Your own behalf, and not on behalf of any Contributor. You must make it absolutely clear that any such warranty, support, indemnity, or liability obligation is offered by You alone, and You hereby agree to indemnify every Contributor for any liability incurred by such Contributor as a result of warranty, support, indemnity or liability terms You offer. You may include additional disclaimers of warranty and limitations of liability specific to any jurisdiction.

4. Inability to Comply Due
to Statute or Regulation

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Software due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be placed in a text file included with all distributions of the Covered Software under

this License. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Termination

5.1. The rights granted under this License will terminate automatically if You fail to comply with any of its terms. However, if You become compliant, then the rights granted under this License from a particular Contributor are reinstated (a) provisionally, unless and until such Contributor explicitly and finally terminates Your grants, and (b) on an ongoing basis, if such Contributor fails to notify You of the non-compliance by some reasonable means prior to 60 days after You have come back into compliance. Moreover, Your grants from a particular Contributor are reinstated on an ongoing basis if such Contributor notifies You of the non-compliance by some reasonable means, this is the first time You have received notice of non-compliance with this License from such Contributor, and You become compliant prior to 30 days after Your receipt of the notice.

5.2. If You initiate litigation against any entity by asserting a patent infringement claim (excluding declaratory judgment actions, counter-claims, and cross-claims) alleging that a Contributor Version directly or indirectly infringes any patent, then the rights granted to You by any and all Contributors for the Covered Software under Section 2.1 of this License shall terminate.

5.3. In the event of termination under Sections 5.1 or 5.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or Your distributors under this License prior to termination shall survive termination.

6. Disclaimer of Warranty

Covered Software is provided under this License on an "as is" basis, without warranty of any kind, either expressed, implied, or statutory, including, without limitation, warranties that the Covered Software is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the Covered Software is with You. Should any Covered Software prove defective in any respect, You (not any Contributor) assume the cost of any necessary servicing, repair, or correction. This disclaimer of warranty constitutes an essential part of this License. No use of any Covered Software is authorized under this License except under this disclaimer.

7. Limitation of Liability

Under no circumstances and under no legal theory, whether tort (including negligence), contract, or otherwise, shall any Contributor, or anyone who distributes Covered Software as permitted above, be liable to You for any direct, indirect, special, incidental, or consequential damages of any character including, without limitation, damages for lost profits, loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses, even if such party shall have been informed of the possibility of such damages. This limitation of liability shall not apply to liability for death or personal injury resulting from such party's negligence to the extent applicable law prohibits such limitation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this exclusion and limitation may not
apply to You.

8. Litigation

Any litigation relating to this License may be brought only in the courts of a jurisdiction where the defendant maintains its principal place of business and such litigation shall be governed by laws of that jurisdiction, without reference to its conflict-of-law provisions. Nothing in this Section shall prevent a party's ability to bring cross-claims or counter-claims.

9. Miscellaneous

This License represents the complete agreement concerning the subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not be used to construe this License against a Contributor.

10. Versions of the License

10.1. New Versions

Mozilla Foundation is the license steward. Except as provided in Section

10.3, no one other than the license steward has the right to modify or publish new versions of this License. Each version will be given a distinguishing version number.

10.2. Effect of New Versions

You may distribute the Covered Software under the terms of the version of the License under which You originally received the Covered Software, or under the terms of any subsequent version published by the license steward.

10.3. Modified Versions

If you create software not governed by this License, and you want to create a new license for such software, you may create and use a modified version of this License if you rename the license and remove any references to the name of the license steward (except to note that such modified license differs from this License).

10.4. Distributing Source Code Form that is Incompatible With Secondary Licenses If You choose to distribute Source Code Form that is Incompatible
With Secondary Licenses under the terms of this version of the License, the notice described in Exhibit B of this License must be attached.

Exhibit A - Source Code Form License Notice

This Source Code Form is subject to the terms of the Mozilla Public License, v. 2.0. If a copy of the MPL was not distributed with this file, You can obtain one at http://mozilla.org/MPL/2.0/.

If it is not possible or desirable to put the notice in a particular file, then You may include the notice in a location (such as a LICENSE file in a relevant directory) where a recipient would be likely to look for such a notice.

You may add additional accurate notices of copyright ownership.

Exhibit B - "Incompatible With Secondary Licenses" Notice

This Source Code Form is "Incompatible With Secondary Licenses", as defined by the Mozilla Public License, v. 2.0.

Blackfriday is distributed under the Simplified BSD License:

> Copyright 2011 Russ Ross
> All rights reserved.
>
> Redistribution and use in source and binary forms, with or without
> modification, are permitted provided that the following conditions

> are met:
>
> 1. Redistributions of source code must retain the above copyright
>   notice, this list of conditions and the following disclaimer.
>
> 2. Redistributions in binary form must reproduce the above
>   copyright notice, this list of conditions and the following
>   disclaimer in the documentation and/or other materials provided with
>   the distribution.
>
> THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
> "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
> LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS
> FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE
> COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
> INCIDENTAL, SPECIAL, EXEMPLARY,
 OR CONSEQUENTIAL DAMAGES (INCLUDING,
> BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
> LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER
> CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
> LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN
> ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
> POSSIBILITY OF SUCH DAMAGE.
This source code was written by the Go contributors.
The master list of contributors is in the main Go distribution,
visible at https://tip.golang.org/CONTRIBUTORS.
Anton Povarov <anton.povarov@gmail.com>
Brian Goff <cpuguy83@gmail.com>
Clayton Coleman <ccoleman@redhat.com>
Denis Smirnov <denis.smirnov.91@gmail.com>
DongYun Kang <ceram1000@gmail.com>
Dwayne Schultz <dschultz@pivotal.io>
Georg Apitz <gapitz@pivotal.io>
Gustav Paul <gustav.paul@gmail.com>
Johan Brandhorst <johan.brandhorst@gmail.com>
John Shahid <jvshahid@gmail.com>
John Tuley <john@tuley.org>
Laurent <laurent@adyoulike.com>
Patrick Lee <patrick@dropbox.com>
Peter Edge <peter.edge@gmail.com>
Roger Johansson <rogeralsing@gmail.com>
Sam Nguyen <sam.nguyen@sendgrid.com>
Sergio Arbeo <serabe@gmail.com>
Stephen J Day <stephen.day@docker.com>
Tamir Duberstein <tamird@gmail.com>
Todd Eisenberger <teisenberger@dropbox.com>
Tormod Erevik Lea <tormodlea@gmail.com>
Vyacheslav Kim <kane@sendgrid.com>

Walter Schulze <awalterschulze@gmail.com>
Alex A. Skinner
Andrew Tunnell-Jones
Ask Bjrn Hansen
Dave Cheney
Dusty Wilson
Marek Majkowski
Peter van Dijk
Omri Bahumi
Alex Sergeyev
James Hartig
// Copyright 2015 Steve Francia <spf@spf13.com>.
//
// Licensed under the Apache License, Version 2.0 (the "License");
// you may not use this file except in compliance with the License.
// You may obtain a copy of the License at
// http://www.apache.org/licenses/LICENSE-2.0
//
// Unless required by applicable law or agreed to in writing, software
// distributed under the License is distributed on an "AS IS" BASIS,
// WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
// See the License for the specific language governing permissions and
// limitations under the License.

// Parts inspired by https://github.com/ryanuber/go-license

package cmd

func initBsdClause2() {
 Licenses["freebsd"] = License{
  Name: "Simplified BSD License",
  PossibleMatches: []string{"freebsd", "simpbsd", "simple bsd", "2-clause bsd",
   "2 clause bsd", "simplified bsd license"},
  Header: `All rights reserved.

Redistribution and use in source and binary forms, with or without
modification,
 are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice,
  this list of conditions and the following disclaimer in the documentation
  and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE

IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.`,
Text: `{{ .copyright }}
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice,
this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice,
this list of conditions and the following disclaimer in the documentation
and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS
BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER
CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,
OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
`,
}
}
All files in this repository are licensed as follows. If you contribute
to this repository, it is assumed that you license your contribution
under the same license unless you state otherwise.

All files Copyright (C) 2015 Canonical Ltd. unless otherwise specified in the file.

This software is licensed under the LGPLv3, included below.

As a special exception to the GNU Lesser General Public License version 3
("LGPL3"), the copyright holders of this Library give you permission to
convey to a third party a Combined Work that links statically or dynamically

to this Library without providing any Minimal Corresponding Source or Minimal Application Code as set out in 4d or providing the installation information set out in section 4e, provided that you comply with the other provisions of LGPL3 and provided that you meet, for the Application the terms and conditions of the license(s) which apply to the Application.

Except as stated in this special exception, the provisions of LGPL3 will continue
to comply in full to this Library. If you modify this Library, you may apply this exception to your version of this Library, but you are not obliged to do so. If you do not wish to do so, delete this exception statement from your version. This exception does not (and cannot) modify any license terms which apply to the Application, with which you must still comply.

GNU LESSER GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and the "GNU
GPL" refers to version 3 of the GNU
General Public License.

"The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An "Application" is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The "Corresponding Application Code" for a Combined Work means the object
code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions
of
this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application

Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

This source code was written by the Go contributors.
The master list of contributors is in the main Go distribution,
visible at http://tip.golang.org/CONTRIBUTORS.

The MIT License (MIT)

Copyright (c) 2014 Simon Eskildsen

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF
OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.

GNU LESSER GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates
the terms and conditions of version 3 of the GNU General Public
License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, "this License" refers to version 3 of the GNU Lesser
General Public License, and the "GNU GPL" refers to version 3 of the GNU
General Public License.

"The Library" refers to a covered work governed by this License,
other than an Application or a Combined Work as defined below.

An "Application" is any work that makes use of an interface provided
by the Library, but which is not otherwise based on the Library.
Defining a subclass of a class defined by
the Library is deemed a mode
of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters,
data structure
layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the

Library is used in it and that the Library and its use are
covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license
document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that,
taken together, effectively do not restrict modification of the
portions of the Library contained in the Combined Work and reverse
engineering for debugging such modifications, if you also do each of
the following:

a) Give prominent notice with each copy of the Combined Work that
the Library is used in it and that the Library and its use are
covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license
document.

c) For a Combined Work that
displays copyright notices during
execution, include the copyright notice for the Library among
these notices, as well as a reference directing the user to the
copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this
License, and the Corresponding Application Code in a form
suitable for, and under terms that permit, the user to
recombine or relink the Application with a modified version of
the Linked Version to produce a modified Combined Work, in the
manner specified by section 6 of the GNU GPL for conveying
Corresponding Source.

1) Use a suitable shared library mechanism for linking with the
Library. A suitable mechanism is one that (a) uses at run time
a copy of the Library already present on the user's computer
system, and (b) will operate properly with a modified version
of the Library that is interface-compatible
with the Linked
Version.

e) Provide Installation Information, but only if you would otherwise
be required to provide such information under section 6 of the
GNU GPL, and only to the extent that such information is

necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the

Library.
MIT License

Copyright (c) 2012-2018 Mat Ryer and Tyler Bunnell

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all
copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT
OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
SOFTWARE.
This is free and unencumbered software released into the public domain.

Anyone is free to copy, modify, publish, use, compile, sell, or
distribute this software, either in source code form or as a compiled
binary, for any purpose, commercial or non-commercial, and by any
means.

In jurisdictions that recognize copyright laws, the author or authors
of this software dedicate any and all copyright interest in the
software to the public domain. We make this dedication for the benefit
of the public at large and to the detriment of our heirs and
successors. We intend this dedication to be an overt act of
relinquishment in perpetuity of all present and future rights to this
software under copyright law.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.
IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY CLAIM, DAMAGES OR
OTHER LIABILITY, WHETHER
IN AN ACTION OF CONTRACT, TORT OR OTHERWISE,
ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR
OTHER DEALINGS IN THE SOFTWARE.

For more information, please refer to <http://unlicense.org>

tomb - support for clean goroutine termination in Go.

Copyright (c) 2010-2011 - Gustavo Niemeyer <gustavo@niemeyer.net>

All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

  * Redistributions of source code must retain the above copyright notice,
    this list of conditions and the following disclaimer.
  * Redistributions in binary form must reproduce the above copyright notice,
    this list of conditions and the following disclaimer in the documentation
    and/or other materials provided with the distribution.
  * Neither the name of the copyright holder nor the names of its
    contributors may be used to endorse or promote products derived from
    this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE
 IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR
PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
/*
Copyright 2014 The Go4 Authors

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

   http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
*/

package legal

```
import (
 "testing"
)

func TestRegisterLicense(t *testing.T) {
 initial := len(licenses)
 RegisterLicense("dummy")
 if initial+1 != len(licenses) {
  t.Fatal("didn't add a license")
 }
}
```

This software is licensed under the LGPLv3, included below.

As a special exception to the GNU Lesser General Public License version 3 ("LGPL3"), the copyright holders of this Library give you permission to convey to a third party a Combined Work that links statically or dynamically to this Library without providing any Minimal Corresponding Source or Minimal Application Code as set out in 4d or providing the installation information set out in section 4e, provided that you comply with the other provisions of LGPL3 and provided that you meet, for the Application the terms and conditions of the license(s) which apply to the Application.

Except as stated in this special exception, the provisions of LGPL3 will continue to comply in full to this Library. If you modify this Library, you may apply this exception to your version of this Library, but you are not obliged to do so. If you do not wish to do so, delete this exception statement from your version. This exception does not (and cannot) modify any
license terms which apply to the Application, with which you must still comply.

GNU LESSER GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and the "GNU GPL" refers to version 3 of the GNU

General Public License.

"The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An "Application" is any work that makes use of an interface provided by the Library,
but which is not otherwise based on the Library.
Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered
work under sections 3 and 4 of this License
without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer

system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities
that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of

the GNU Lesser General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial
revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this
License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their

Contribution(s) alone or by combination of their Contribution(s)
with the Work to which such Contribution(s) was submitted. If You
institute patent litigation against any entity (including a
cross-claim or counterclaim in a lawsuit) alleging that the Work
or a Contribution incorporated within the Work constitutes direct
or contributory patent infringement, then any patent licenses
granted to You under this License for that Work shall terminate
as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute
copies of the
Work or Derivative Works thereof in any medium, with or without
modifications, and in Source or Object form, provided that You
meet the following conditions:

(a) You must give any other recipients of the Work or
Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices
stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works
that You distribute, all copyright, patent, trademark, and
attribution notices from the Source form of the Work,
excluding those notices that do not pertain to any part of
the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its
distribution, then any Derivative Works that You distribute must
include a readable copy of the attribution notices contained
within such NOTICE file, excluding
those notices that do not
pertain to any part of the Derivative Works, in at least one
of the following places: within a NOTICE text file distributed
as part of the Derivative Works; within the Source form or
documentation, if provided along with the Derivative Works; or,
within a display generated by the Derivative Works, if and
wherever such third-party notices normally appear. The contents
of the NOTICE file are for informational purposes only and
do not modify the License. You may add Your own attribution
notices within Derivative Works that You distribute, alongside
or as an addendum to the NOTICE text from the Work, provided
that such additional attribution notices cannot be construed
as modifying the License.

You may add Your own copyright statement to Your modifications and
may provide additional or different license terms and conditions

for use, reproduction, or distribution of Your modifications, or
for any such Derivative Works as a whole, provided Your use,
reproduction, and distribution of the Work otherwise complies with
the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise,
any Contribution intentionally submitted for inclusion in the Work
by You to the Licensor shall be under the terms and conditions of
this License, without any additional terms or conditions.
Notwithstanding the above, nothing herein shall supersede or modify
the terms of any separate license agreement you may have executed
with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade
names, trademarks, service marks, or product names of the Licensor,
except as required for reasonable and customary use in describing the
origin of the Work and reproducing the
content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or
agreed to in writing, Licensor provides the Work (and each
Contributor provides its Contributions) on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
implied, including, without limitation, any warranties or conditions
of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A
PARTICULAR PURPOSE. You are solely responsible for determining the
appropriateness of using or redistributing the Work and assume any
risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory,
whether in tort (including negligence), contract, or otherwise,
unless required by applicable law (such as deliberate and grossly
negligent acts) or agreed to in writing, shall any Contributor be
liable to You for damages, including any direct,
indirect, special,
incidental, or consequential damages of any character arising as a
result of this License or out of the use or inability to use the
Work (including but not limited to damages for loss of goodwill,
work stoppage, computer failure or malfunction, or any and all
other commercial damages or losses), even if such Contributor
has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing
the Work or Derivative Works thereof, You may choose to offer,
and charge a fee for, acceptance of support, warranty, indemnity,
or other liability obligations and/or rights consistent with this
License. However, in accepting such obligations, You may act only
on Your own behalf and on Your sole responsibility, not on behalf

```
    of any other Contributor, and only if You agree to indemnify,
    defend, and hold each Contributor harmless for any liability
     incurred by, or claims asserted against, such Contributor by reason
    of your accepting any such warranty or additional liability.
// Copyright  2015 Steve Francia <spf@spf13.com>.
//
// Licensed under the Apache License, Version 2.0 (the "License");
// you may not use this file except in compliance with the License.
// You may obtain a copy of the License at
// http://www.apache.org/licenses/LICENSE-2.0
//
// Unless required by applicable law or agreed to in writing, software
// distributed under the License is distributed on an "AS IS" BASIS,
// WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
// See the License for the specific language governing permissions and
// limitations under the License.

// Parts inspired by https://github.com/ryanuber/go-license

package cmd

func initMit() {
 Licenses["mit"] = License{
  Name:           "MIT License",
  PossibleMatches: []string{"mit"},
  Header: `
Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including
 without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.`,
  Text: `The MIT License (MIT)

{{ .copyright }}
```

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation
files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.
`,
}
}
The MIT License (MIT)

Copyright (c) 2014 Brian Goff

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all
copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN
CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
SOFTWARE.
The MIT License (MIT)

Copyright (c) 2013 Mitchell Hashimoto

Permission is hereby granted, free of charge, to any person obtaining a copy

of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT
OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.
Copyright (C) 2014 by Oleku Konko

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE
SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.
All files in this repository are licensed as follows. If you contribute
to this repository, it is assumed that you license your contribution
under the same license unless you state otherwise.

All files Copyright (C) 2012-2016 Canonical Ltd. unless otherwise specified in the file.

This software is licensed under the LGPLv3, included below.

As a special exception to the GNU Lesser General Public License version 3
("LGPL3"), the copyright holders of this Library give you permission to
convey to a third party a Combined Work that links statically or dynamically

to this Library without providing any Minimal Corresponding Source or Minimal Application Code as set out in 4d or providing the installation information set out in section 4e, provided that you comply with the other provisions of LGPL3 and provided that you meet, for the Application the terms and conditions of the license(s) which apply to the Application.

Except as stated in this special exception, the provisions of LGPL3 will continue
to comply in full to this Library. If you modify this Library, you may apply this exception to your version of this Library, but you are not obliged to do so. If you do not wish to do so, delete this exception statement from your version. This exception does not (and cannot) modify any license terms which apply to the Application, with which you must still comply.

GNU LESSER GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and
the "GNU GPL" refers to version 3 of the GNU General Public License.

"The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An "Application" is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The "Corresponding Application Code" for a Combined Work means the object
code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of
this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application

Code. If you use option 4d1, you must provide the
Installation
Information in the manner specified by section 6 of the GNU GPL
for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the
Library side by side in a single library together with other library
facilities that are not Applications and are not covered by this
License, and convey such a combined library under terms of your
choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based
on the Library, uncombined with any other library facilities,
conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it
is a work based on the Library, and explaining where to find the
accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions
of the GNU Lesser General Public License
from time to time. Such new
versions will be similar in spirit to the present version, but may
differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the
Library as you received it specifies that a certain numbered version
of the GNU Lesser General Public License "or any later version"
applies to it, you have the option of following the terms and
conditions either of that published version or of any later version
published by the Free Software Foundation. If the Library as you
received it does not specify a version number of the GNU Lesser
General Public License, you may choose any version of the GNU Lesser
General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide
whether future versions of the GNU Lesser General Public License shall
apply, that proxy's public statement of acceptance of any version is
permanent authorization for you to choose that
version for the
Library.
// Copyright 2015 Steve Francia <spf@spf13.com>.
//
// Licensed under the Apache License, Version 2.0 (the "License");

```
// you may not use this file except in compliance with the License.
// You may obtain a copy of the License at
// http://www.apache.org/licenses/LICENSE-2.0
//
// Unless required by applicable law or agreed to in writing, software
// distributed under the License is distributed on an "AS IS" BASIS,
// WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
// See the License for the specific language governing permissions and
// limitations under the License.

// Parts inspired by https://github.com/ryanuber/go-license

package cmd

func initBsdClause3() {
 Licenses["bsd"] = License{
  Name:            "NewBSD",
  PossibleMatches: []string{"bsd", "newbsd", "3 clause bsd", "3-clause bsd"},
  Header: `All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
 are met:

1. Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice,
  this list of conditions and the following disclaimer in the documentation
  and/or other materials provided with the distribution.

3. Neither the name of the copyright holder nor the names of its contributors
  may be used to endorse or promote products derived from this software
  without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE
LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE
 GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.`,
  Text: `{{ .copyright }}
```

All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice,
  this list of conditions and the following disclaimer in the documentation
  and/or other materials provided with the distribution.

3. Neither the name of the copyright holder nor the names of its contributors
  may be used to endorse or promote products derived from this software
   without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER
CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,
OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
`,
 }
}
MIT License

Copyright (c) 2015 Dmitri Shuralyov

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all
copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,

OUT OF OR IN CONNECTION
WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
SOFTWARE.
Copyright (c) 2012-2018 The Gorilla Authors. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are
met:

* Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above
copyright notice, this list of conditions and the following disclaimer
in the documentation and/or other materials provided with the
distribution.
* Neither the name of Google Inc. nor the names of its
contributors may be used to endorse or promote products derived from
this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT
OWNER
OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
ISC License

Copyright (c) 2012-2016 Dave Collins <dave@davec.name>

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES
WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR
ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF
OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.
The following files were ported to Go from C files of libyaml, and thus
are still covered by their original copyright and license:

apic.go
emitterc.go
parserc.go
readerc.go
scannerc.go
writerc.go
yamlh.go
yamlprivateh.go

Copyright (c) 2006 Kirill Simonov

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS
FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the

direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License,
each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute
copies of the
Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding

those notices that do not
pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions

for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the
content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise,

```
    unless required by applicable law (such as deliberate and grossly
    negligent acts) or agreed to in writing, shall any Contributor be
    liable to You for damages, including any direct,
 indirect, special,
    incidental, or consequential damages of any character arising as a
    result of this License or out of the use or inability to use the
    Work (including but not limited to damages for loss of goodwill,
    work stoppage, computer failure or malfunction, or any and all
    other commercial damages or losses), even if such Contributor
    has been advised of the possibility of such damages.

  9. Accepting Warranty or Additional Liability. While redistributing
    the Work or Derivative Works thereof, You may choose to offer,
    and charge a fee for, acceptance of support, warranty, indemnity,
    or other liability obligations and/or rights consistent with this
    License. However, in accepting such obligations, You may act only
    on Your own behalf and on Your sole responsibility, not on behalf
    of any other Contributor, and only if You agree to indemnify,
    defend, and hold each Contributor harmless for any liability

    incurred by, or claims asserted against, such Contributor by reason
    of your accepting any such warranty or additional liability.
// Copyright  2015 Steve Francia <spf@spf13.com>.
//
// Licensed under the Apache License, Version 2.0 (the "License");
// you may not use this file except in compliance with the License.
// You may obtain a copy of the License at
// http://www.apache.org/licenses/LICENSE-2.0
//
// Unless required by applicable law or agreed to in writing, software
// distributed under the License is distributed on an "AS IS" BASIS,
// WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
// See the License for the specific language governing permissions and
// limitations under the License.

// Parts inspired by https://github.com/ryanuber/go-license

package cmd

func initApache2() {
 Licenses["apache"] = License{
  Name:            "Apache 2.0",
  PossibleMatches: []string{"apache", "apache20", "apache 2.0", "apache2.0", "apache-2.0"},
  Header: `
Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may
```

obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.`,
Text: `
Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction,
and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by
the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all

other entities that control, are controlled by, or are under common
control with that entity. For the purposes of this definition,
"control" means (i) the power, direct or indirect, to cause the
direction or management of such entity, whether by contract or
otherwise, or (ii) ownership of fifty percent (50%) or more of the
outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity
exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications,
including but not limited to software source code, documentation
source, and configuration files.

"Object" form shall mean any form resulting from mechanical
transformation or translation of a Source form, including but
not limited to compiled object code, generated documentation,
and conversions to other media types.

"Work" shall mean
the work of authorship, whether in Source or
Object form, made available under the License, as indicated by a

copyright notice that is included in or attached to the work
(an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the
Work by the copyright owner
or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each
Contributor hereby grants to You a perpetual,
worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against

any entity (including a
cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices
from the Source form of the Work,
excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise,
any Contribution intentionally submitted for inclusion in the Work
by You to the Licensor shall be under the terms and conditions of
this License, without any additional terms or conditions.
Notwithstanding the above, nothing herein shall supersede
or modify
the terms of any separate license agreement you may have executed
with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade
names, trademarks, service marks, or product names of the Licensor,
except as required for reasonable and customary use in describing the
origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or
agreed to in writing, Licensor provides the Work (and each
Contributor provides its Contributions) on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
implied, including, without limitation, any warranties or conditions
of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A
PARTICULAR PURPOSE. You are solely responsible for determining the
appropriateness of using or redistributing the Work and assume any
risks
associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory,
whether in tort (including negligence), contract, or otherwise,
unless required by applicable law (such as deliberate and grossly
negligent acts) or agreed to in writing, shall any Contributor be
liable to You for damages, including any direct, indirect, special,
incidental, or consequential damages of any character arising as a
result of this License or out of the use or inability to use the
Work (including but not limited to damages for loss of goodwill,
work stoppage, computer failure or malfunction, or any and all
other commercial damages or losses), even if such Contributor
has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing
the Work or Derivative Works thereof, You may choose to offer,
and charge a fee
for, acceptance of support, warranty, indemnity,
or other liability obligations and/or rights consistent with this
License. However, in accepting such obligations, You may act only
on Your own behalf and on Your sole responsibility, not on behalf
of any other Contributor, and only if You agree to indemnify,
defend, and hold each Contributor harmless for any liability
incurred by, or claims asserted against, such Contributor by reason

of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following
boilerplate notice, with the fields enclosed by brackets "[]"
replaced with your own identifying information. (Don't include
the brackets!) The text should be enclosed in the appropriate
comment syntax for the file format. We also recommend that a
file or class name
and description of purpose be included on the
same "printed page" as the copyright notice for easier
identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
`,
}
}
Copyright 2009 The Go Authors. All rights reserved. Use of this source code
is governed by a BSD-style license that can be found in the LICENSE file.
Extensions of the original work are copyright (c) 2011 Miek Gieben

Copyright 2011 Miek Gieben. All rights reserved. Use of this source code is
governed by a BSD-style license that can be found in the LICENSE file.

Copyright 2014 CloudFlare. All rights reserved. Use of this source code is
governed by a BSD-style license that can be found in the LICENSE file.
The MIT License (MIT)

Copyright (c) 2013 Ben Johnson

Permission is hereby granted, free of charge, to any person obtaining a copy of
this software and associated documentation files (the "Software"), to deal in
the Software without restriction, including without limitation the rights to

use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of
the Software, and to permit persons to whom the Software is furnished to do so,
subject to the following conditions:

The above copyright notice and this permission notice shall be included in all
copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION
WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
Contributors to log15:

- Aaron L
- Alan Shreve
- Chris Hines
- Ciaran Downey
- Dmitry Chestnykh
- Evan Shaw
- Pter Szilgyi
- Trevor Gattis
- Vincent Vanackere
The MIT License (MIT)

Copyright (c) 2013-2014 Florian Schlachter

Permission is hereby granted, free of charge, to any person obtaining a copy of
this software and associated documentation files (the "Software"), to deal in
the Software without restriction, including without limitation the rights to
use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of
the Software, and to permit persons to whom the Software is furnished to do so,
subject to the following conditions:

The above copyright notice and this permission notice shall be included in all
copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN
CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
Copyright (c) 2012-2016 Jos Carlos Nieto, https://menteslibres.net/xiam

Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE
LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
OF CONTRACT, TORT OR OTHERWISE, ARISING
FROM, OUT OF OR IN CONNECTION
WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
Copyright (c) 2009 The Go Authors. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are
met:

* Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above
copyright notice, this list of conditions and the following disclaimer
in the documentation and/or other materials provided with the
distribution.
* Neither the name of Google Inc. nor the names of its
contributors may be used to endorse or promote products derived from
this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT
OWNER
OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This licence applies to the following files:

* filepath/stdlib.go
* filepath/stdlibmatch.go

Copyright (c) 2010 The Go Authors. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are
met:

  * Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
  * Redistributions in binary form must reproduce the above
copyright notice, this list of conditions and the following disclaimer
in the documentation and/or other materials provided with the
distribution.
  * Neither the name of Google Inc. nor the names of its
contributors may be used to endorse or promote products derived from
this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY
 AND FITNESS FOR
A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT
OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
mgo - MongoDB driver for Go

Copyright (c) 2010-2013 - Gustavo Niemeyer <gustavo@niemeyer.net>

All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this
  list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice,
  this list of conditions and the following disclaimer in the documentation
  and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING,
BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
BSON library for Go

Copyright (c) 2010-2012 - Gustavo Niemeyer <gustavo@niemeyer.net>

All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this
   list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice,
   this list of conditions and the following disclaimer in the documentation
   and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING,
BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
Paul Borman <borman@google.com>
package cmd

```
func initLgpl() {
 Licenses["lgpl"] = License{
  Name:            "GNU Lesser General Public License",
  PossibleMatches: []string{"lgpl", "lesser gpl", "gnu lgpl"},
  Header: `
```
This program is free software: you can redistribute it and/or modify
it under the terms of the GNU Lesser General Public License as published by
the Free Software Foundation, either version 3 of the License, or

(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License
along with this program. If not, see <http://www.gnu.org/licenses/>.`,
 Text: `   GNU LESSER GENERAL PUBLIC LICENSE
                       Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
 Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

 This version of the GNU Lesser General Public License incorporates
the terms and conditions of version 3 of the GNU General Public
License, supplemented by the additional permissions listed below.

 0. Additional Definitions.

 As used herein, "this License" refers to version 3 of the GNU Lesser
General Public License, and the "GNU GPL" refers to version 3 of the GNU
General Public License.

 "The Library" refers to a covered work governed by this License,
other than an Application or a Combined Work as defined below.

 An "Application" is any work that makes use of an interface provided
by the Library, but which is not otherwise based on the Library.
Defining a subclass of a class defined by the Library is deemed a mode
of using an interface provided by the Library.

 A "Combined Work" is a work produced by combining or linking an
Application with the Library.
 The particular version of the Library
with which the Combined Work was made is also called the "Linked
Version".

 The "Minimal Corresponding Source" for a Combined Work means the
Corresponding Source for the Combined Work, excluding any source code
for portions of the Combined Work that, considered in isolation, are
based on the Application, and not on the Linked Version.

 The "Corresponding Application Code" for a Combined Work means the
object code and/or source code for the Application, including any data

and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that
uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a) Give
prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of

the following:

a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library

facilities that are not Applications and are not covered by this
License, and convey such a combined library under terms of your
choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based
on the Library, uncombined
with any other library facilities,
conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it
is a work based on the Library, and explaining where to find the
accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions
of the GNU Lesser General Public License from time to time. Such new
versions will be similar in spirit to the present version, but may
differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the
Library as you received it specifies that a certain numbered version
of the GNU Lesser General Public License "or any later version"
applies to it, you have the option of following the terms and
conditions either of that published version or of any later version
published by the Free Software Foundation. If the Library as you
received
it does not specify a version number of the GNU Lesser
General Public License, you may choose any version of the GNU Lesser
General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide
whether future versions of the GNU Lesser General Public License shall
apply, that proxy's public statement of acceptance of any version is
permanent authorization for you to choose that version for the
Library.`,
}
}
MIT License

Copyright (c) 2017 HashiCorp

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all
copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION
WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
SOFTWARE.
Copyright (c) Yasuhiro MATSUMOTO <mattn.jp@gmail.com>

MIT License (Expat)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING
FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition,

"control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and

subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License,
each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute
copies of the
Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding

those notices that do not
pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions

for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the
content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise,

unless required by applicable law (such as deliberate and grossly
negligent acts) or agreed to in writing, shall any Contributor be
liable to You for damages, including any direct,
indirect, special,
incidental, or consequential damages of any character arising as a
result of this License or out of the use or inability to use the
Work (including but not limited to damages for loss of goodwill,
work stoppage, computer failure or malfunction, or any and all
other commercial damages or losses), even if such Contributor
has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing
the Work or Derivative Works thereof, You may choose to offer,
and charge a fee for, acceptance of support, warranty, indemnity,
or other liability obligations and/or rights consistent with this
License. However, in accepting such obligations, You may act only
on Your own behalf and on Your sole responsibility, not on behalf
of any other Contributor, and only if You agree to indemnify,
defend, and hold each Contributor harmless for any liability
incurred by, or claims asserted against, such Contributor by reason
of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following
boilerplate notice, with the fields enclosed by brackets "{}"
replaced with your own identifying information. (Don't include
the brackets!) The text should be enclosed in the appropriate
comment syntax for the file format. We also recommend that a
file or class name and description of purpose be included on the
same "printed page" as the copyright notice for easier
identification within third-party archives.

Copyright {yyyy} {name of copyright owner}

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.

The author disclaims copyright to this source code. In place of
a legal notice, here is a blessing:

 * May you do good and not evil.
 * May you find forgiveness for yourself and forgive others.
 * May you share freely, never taking more than you give.
Copyright (c) 2012 The Go Authors. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are
met:

  * Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
  * Redistributions in binary form must reproduce the above
copyright notice, this list of conditions and the following disclaimer
in the documentation and/or other materials provided with the
distribution.
  * Neither the name of Google Inc. nor the names of its
contributors may be used to endorse or promote products derived from
this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT
OWNER
 OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
This software is licensed under the LGPLv2.1, included below.

As a special exception to the GNU Lesser General Public License version 2.1
("LGPL2.1"), the copyright holders of this Library give you permission to
convey to a third party a Combined Work that links statically or dynamically
to this Library without providing any Minimal Corresponding Source or
Minimal Application Code or providing the installation information,
provided that you comply with the other provisions of LGPL2.1
and provided that you meet, for the Application the terms and conditions
of the license(s) which apply to the Application.

Except as stated in this special exception, the provisions of LGPL2.1 will
continue to comply in full to this Library. If you modify this Library, you
may apply this exception to your version of this Library, but you are not

obliged to do so. If you do not wish to do so, delete this exception statement from your version. This exception does not (and cannot) modify any license terms which
apply to the Application, with which you must still
comply.

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically
libraries--of the
Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify
it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected
by problems that might be
introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original
library. The ordinary
General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many

libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a

portion of it, either verbatim
or with modifications and/or translated
straightforwardly into another language. (Hereinafter, translation is
included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for
making modifications to it. For a library, complete source code means
all the source code for all modules it contains, plus any associated
interface definition files, plus the scripts used to control compilation
and installation of the library.

Activities other than copying, distribution and modification are not
covered by this License; they are outside its scope. The act of
running a program using the Library is not restricted, and output from
such a program is covered only if its contents constitute a work based
on the Library (independent of the use of the Library in a tool for
writing it). Whether that is true depends on what the Library does
and what the program that uses the Library does.

1. You may copy and distribute verbatim copies
of the Library's
complete source code as you receive it, in any medium, provided that
you conspicuously and appropriately publish on each copy an
appropriate copyright notice and disclaimer of warranty; keep intact
all the notices that refer to this License and to the absence of any
warranty; and distribute a copy of this License along with the
Library.

You may charge a fee for the physical act of transferring a copy,
and you may at your option offer warranty protection in exchange for a
fee.

2. You may modify your copy or copies of the Library or any portion
of it, thus forming a work based on the Library, and copy and
distribute such modifications or work under the terms of Section 1
above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices
stating that you changed the files and the date of any change.

c) You must cause the whole of the work
to be licensed at no
charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a
table of data to be supplied by an application program that uses

the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable
sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope
of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6.

Any executables containing that work also fall under Section 6,
whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or
link a "work that uses the Library" with the Library to produce a
work containing portions of the Library, and distribute that work
under terms of your choice, provided that the terms permit
modification of the work for the customer's own use and reverse
engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the
Library is used in it and that the Library and its use are covered by
this License. You must supply a copy of this License. If the work
during execution displays copyright notices, you must include the
copyright notice for the Library among them, as well as a reference
directing the user to the copy of this
License. Also, you must do one
of these things:

a) Accompany the work with the complete corresponding
machine-readable source code for the Library including whatever
changes were used in the work (which must be distributed under
Sections 1 and 2 above); and, if the work is an executable linked
with the Library, with the complete machine-readable "work that
uses the Library", as object code and/or source code, so that the
user can modify the Library and then relink to produce a modified
executable containing the modified Library. (It is understood
that the user who changes the contents of definitions files in the
Library will not necessarily be able to recompile the application
to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the
Library. A suitable mechanism is one that (1) uses at run time a
copy of the library already present on the user's computer system,
rather than copying
library functions into the executable, and (2)
will operate properly with a modified version of the library, if
the user installs one, as long as the modified version is
interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at
least three years, to give the same user the materials
specified in Subsection 6a, above, for a charge no more
than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy
from a designated place, offer equivalent access to copy the above
specified materials from the same place.

e) Verify that the user has already received a copy of these
materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the
Library" must include any data and utility programs needed for
reproducing the executable from it. However, as a special exception,
the
materials to be distributed need not include anything that is
normally distributed (in either source or binary form) with the major
components (compiler, kernel, and so on) of the operating system on
which the executable runs, unless that component itself accompanies
the executable.

It may happen that this requirement contradicts the license
restrictions of other proprietary libraries that do not normally
accompany the operating system. Such a contradiction means you cannot
use both them and the Library together in an executable that you
distribute.

7. You may place library facilities that are a work based on the
Library side-by-side in a single library together with other library
facilities not covered by this License, and distribute such a combined
library, provided that the separate distribution of the work based on
the Library and of the other library facilities is otherwise
permitted, and provided that you do these two things:

a) Accompany the combined library with
a copy of the same work
based on the Library, uncombined with any other library
facilities. This must be distributed under the terms of the
Sections above.

b) Give prominent notice with the combined library of the fact
that part of it is a work based on the Library, and explaining
where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute
the Library except as expressly provided under this License. Any
attempt otherwise to copy, modify, sublicense, link with, or
distribute the Library is void, and will automatically terminate your
rights under this License. However, parties who have received copies,
or rights, from you under this License will not have their licenses
terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not
signed it. However, nothing else grants you permission to modify or
distribute the Library

or its derivative works. These actions are
prohibited by law if you do not accept this License. Therefore, by
modifying or distributing the Library (or any work based on the
Library), you indicate your acceptance of this License to do so, and
all its terms and conditions for copying, distributing or modifying
the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the
Library), the recipient automatically receives a license from the
original licensor to copy, distribute, link with or modify the Library
subject to these terms and conditions. You may not impose any further
restrictions on the recipients' exercise of the rights granted herein.
You are not responsible for enforcing compliance by third parties with
this License.

11. If, as a consequence of a court judgment or allegation of patent
infringement or for any other reason (not limited to patent issues),
conditions are imposed on you (whether by court order, agreement or
otherwise)
that contradict the conditions of this License, they do not
excuse you from the conditions of this License. If you cannot
distribute so as to satisfy simultaneously your obligations under this
License and any other pertinent obligations, then as a consequence you
may not distribute the Library at all. For example, if a patent
license would not permit royalty-free redistribution of the Library by
all those who receive copies directly or indirectly through you, then
the only way you could satisfy both it and this License would be to
refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any
particular circumstance, the balance of the section is intended to apply,
and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any
patents or other property right claims or to contest validity of any
such claims; this section has the sole purpose
of protecting the
integrity of the free software distribution system which is
implemented by public license practices. Many people have made
generous contributions to the wide range of software distributed
through that system in reliance on consistent application of that
system; it is up to the author/donor to decide if he or she is willing
to distribute software through any other system and a licensee cannot
impose that choice.

This section is intended to make thoroughly clear what is believed to
be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU

FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest
to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software

Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the
library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!
// Copyright 2015 Steve Francia <spf@spf13.com>.
//
// Licensed under the Apache License, Version 2.0 (the "License");
// you may not use this file except in compliance with the License.
// You may obtain a copy of the License at
// http://www.apache.org/licenses/LICENSE-2.0
//
// Unless required by applicable law or agreed to in writing, software
// distributed under the License is distributed on an "AS IS" BASIS,
// WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
// See the License for the specific language governing permissions and
// limitations under the License.

// Parts inspired by https://github.com/ryanuber/go-license

package cmd

func initGpl3() {
 Licenses["gpl3"] = License{
  Name: "GNU General Public License 3.0",
  PossibleMatches: []string{"gpl3", "gplv3", "gpl", "gnu gpl3", "gnu gpl"},
  Header: `
This program is free software: you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the
 Free Software Foundation, either version 3 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program. If not, see <http://www.gnu.org/licenses/>.`,
  Text: `   GNU GENERAL PUBLIC LICENSE
                       Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified

versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render
the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly
or secondarily liable for
infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the

public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent
item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific
operating system
(if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically

linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention

is
effected by exercising rights under this License with respect to
the covered work, and you disclaim any intention to limit operation or
modification of the work as a means of enforcing, against the work's
users, your or third parties' legal rights to forbid circumvention of
technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you
receive it, in any medium, provided that you conspicuously and
appropriately publish on each copy an appropriate copyright notice;
keep intact all notices stating that this License and any
non-permissive terms added in accord with section 7 apply to the code;
keep intact all notices of the absence of any warranty; and give all
recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey,
and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based
on the Program, or the modifications to
produce it from the Program, in the form of source code under the
terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified
it, and giving a relevant date.

b) The work must carry prominent notices stating that it is
released under this License and any conditions added under section
7. This requirement modifies the requirement in section 4 to
"keep intact all notices".

c) You must license the entire work, as a whole, under this
License to anyone who comes into possession of a copy. This
License will therefore apply, along with any applicable section 7
additional terms, to the whole of the work, and all its parts,
regardless of how they are packaged. This License gives no
permission to license the work in any other way, but it does not
invalidate such permission if you have separately received it.

d)
If the work has interactive user interfaces, each must display
Appropriate Legal Notices; however, if the Program has interactive
interfaces that do not display Appropriate Legal Notices, your
work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to

copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply

if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed,
and Installation Information provided,
in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions
may be written to require their own
removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or
requiring that modified versions of such material be marked in
reasonable ways as different from the original version; or

d) Limiting the use for
publicity purposes of names of licensors or
authors of the material; or

e) Declining to grant rights under trademark law for use of some
trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that
material by anyone who conveys the material (or modified versions of
it) with contractual assumptions of liability to the recipient, for
any liability that these contractual assumptions directly impose on
those licensors and authors.

All other non-permissive additional terms are considered "further
restrictions" within the meaning of section 10. If the Program as you
received it, or any part of it, contains a notice stating that it is
governed by this License along with a term that is a further
restriction, you may remove that term. If a license document contains
a further restriction but permits relicensing or conveying under this
License, you may add to a covered work material governed by the terms
of that
license document, provided that the further restriction does
not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you
must place, in the relevant source files, a statement of the
additional terms that apply to those files, or a notice indicating
where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the
form of a separately written license, or stated as exceptions;
the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly
provided under this License. Any attempt otherwise to propagate or
modify it is void, and will automatically terminate your rights under
this License (including any patent licenses granted under the third
paragraph of section 11).

However, if you cease all violation of this License, then your
license from a particular copyright holder is reinstated (a)

provisionally, unless and until the
copyright holder explicitly and
finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive
or
run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of
a covered
work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have

actual knowledge that, but for the patent license, your conveying the covered work
in a country, or your recipient's use of the covered work
in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under
which you make payment
to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey
a
covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you
to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the

GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>
This program comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if
you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what you want to do, use the GNU Lesser General
Public License instead of this License. But first, please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.
`,
}
}
package cmd

func initAgpl() {
Licenses["agpl"] = License{
Name: "GNU Affero General Public License",
PossibleMatches: []string{"agpl", "affero gpl", "gnu agpl"},
Header: `
This program is free software: you can redistribute it and/or modify
it under the terms of the GNU Affero General Public License as published by
the Free Software Foundation, either version 3 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of

MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU Affero General Public License for more details.

You should have received a copy of the GNU Affero General Public License
along with this program. If not, see <http://www.gnu.org/licenses/>.`,
Text: ` GNU AFFERO GENERAL PUBLIC LICENSE
Version 3, 19 November 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU Affero General Public License is a free, copyleft license for
software and other kinds of works, specifically designed to ensure
cooperation with the community in the case of network server software.

The licenses for most software and other practical works are designed
to take away your freedom to share and change the works. By contrast,
our General Public Licenses are intended to guarantee your freedom to
share and change all versions of a program--to make sure it remains free
software for all its users.

When we speak of free software, we are referring to freedom, not
price. Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
them if you wish), that you receive source code or can get it if you
want it, that you can change
the software or use pieces of it in new
free programs, and that you know you can do these things.

Developers that use our General Public Licenses protect your rights
with two steps: (1) assert copyright on the software, and (2) offer
you this License which gives you legal permission to copy, distribute
and/or modify the software.

A secondary benefit of defending all users' freedom is that
improvements made in alternate versions of the program, if they
receive widespread use, become available for other developers to
incorporate. Many developers of free software are heartened and
encouraged by the resulting cooperation. However, in the case of
software used on network servers, this result may fail to come about.
The GNU General Public License permits making a modified version and
letting the public access it on a server without ever releasing its
source code to the public.

The GNU Affero General Public License is designed specifically to

ensure that, in such cases, the modified
source code becomes available
to the community. It requires the operator of a network server to
provide the source code of the modified version running there to the
users of that server. Therefore, public use of a modified version, on
a publicly accessible server, gives the public access to the source
code of the modified version.

An older license, called the Affero General Public License and
published by Affero, was designed to accomplish similar goals. This is
a different license, not a version of the Affero GPL, but Affero has
released a new version of the Affero GPL which permits relicensing under
this license.

The precise terms and conditions for copying, distribution and
modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU Affero General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of
works, such as semiconductor masks.

"The Program" refers to
any copyrightable work licensed under this
License. Each licensee is addressed as "you". "Licensees" and
"recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work
in a fashion requiring copyright permission, other than the making of an
exact copy. The resulting work is called a "modified version" of the
earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based
on the Program.

To "propagate" a work means to do anything with it that, without
permission, would make you directly or secondarily liable for
infringement under applicable copyright law, except executing it on a
computer or modifying a private copy. Propagation includes copying,
distribution (with or without modification), making available to the
public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other
parties to make or receive

copies. Mere interaction with a user through
a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices"
to the extent that it includes a convenient and prominently visible
feature that (1) displays an appropriate copyright notice, and (2)
tells the user that there is no warranty for the work (except to the
extent that warranties are provided), that licensees may convey the
work under this License, and how to view a copy of this License. If
the interface presents a list of user commands or options, such as a
menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work
for making modifications to it. "Object code" means any non-source
form of a work.

A "Standard Interface" means an interface that either is an official
standard defined by a recognized standards body, or, in the case of
interfaces specified for a particular
programming language, one that
is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other
than the work as a whole, that (a) is included in the normal form of
packaging a Major Component, but which is not part of that Major
Component, and (b) serves only to enable use of the work with that
Major Component, or to implement a Standard Interface for which an
implementation is available to the public in source code form. A
"Major Component", in this context, means a major essential component
(kernel, window system, and so on) of the specific operating system
(if any) on which the executable work runs, or a compiler used to
produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all
the source code needed to generate, install, and (for an executable
work) run the object code and to modify the work, including scripts to
control those activities.
However, it does not include the work's
System Libraries, or general-purpose tools or generally available free
programs which are used unmodified in performing those activities but
which are not part of the work. For example, Corresponding Source
includes interface definition files associated with source files for
the work, and the source code for shared libraries and dynamically
linked subprograms that the work is specifically designed to require,
such as by intimate data communication or control flow between those
subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's

users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which

are not combined with it such as to form a larger program,
in or on a volume of a storage or distribution medium, is called an
"aggregate" if the compilation and its resulting copyright are not
used to limit the access or legal rights of the compilation's users
beyond what the individual works permit. Inclusion of a covered work
in an aggregate does not cause this License to apply to the other
parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms
of sections 4 and 5, provided that you also convey the
machine-readable Corresponding Source under the terms of this License,
in one of these ways:

a) Convey the object code in, or embodied in, a physical product
(including a physical distribution medium), accompanied by the
Corresponding Source fixed on a durable physical medium
customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product
(including
a physical distribution medium), accompanied by a
written offer, valid for at least three years and valid for as
long as you offer spare parts or customer support for that product
model, to give anyone who possesses the object code either (1) a
copy of the Corresponding Source for all the software in the
product that is covered by this License, on a durable physical
medium customarily used for software interchange, for a price no
more than your reasonable cost of physically performing this
conveying of source, or (2) access to copy the
Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the
written offer to provide the Corresponding Source. This
alternative is allowed only occasionally and noncommercially, and
only if you received the object code with such an offer, in accord
with subsection 6b.

d) Convey the object code by offering access from a designated
place (gratis or for a charge), and offer equivalent access to the
Corresponding Source in the same way through the same place at no
further charge. You need not require recipients to copy the
Corresponding Source along with the object code. If the place to
copy the object code is a network server, the Corresponding Source
may be on a different server (operated by you or a third party)
that supports equivalent copying facilities, provided you maintain
clear directions next to the object code saying where to find the

Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use
of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability
to install
modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a

requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making
exceptions from one or more of its conditions.
Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of
that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation

(including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but
do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding
Source of the work is not available for anyone
to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Remote Network Interaction; Use with the GNU General Public License.

Notwithstanding any other provision of this License, if you modify the Program, your modified version must prominently offer all users interacting with it remotely through a computer network (if your version supports such interaction) an opportunity to receive the Corresponding

Source of your version by providing access to the Corresponding Source from a network server at no charge, through some standard or customary means of facilitating copying of software. This Corresponding Source shall include the Corresponding Source for any work covered by version 3 of the GNU General Public License that is incorporated pursuant to the following paragraph.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU General Public License into a single combined work,
and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the work with which it is combined will remain governed by version 3 of the GNU General Public License.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU Affero General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU Affero General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU Affero General Public License, you may choose any
version ever published
by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU Affero General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY

OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD
THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF
ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute
waiver of all civil liability in connection with the
Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU

Affero General Public License as published by
the Free Software Foundation, either version 3 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU Affero General Public License for more details.

You should have received a copy of the GNU Affero General Public License
along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If your software can interact with users remotely through a computer
network, you should also make sure that it provides a way for users to
get its source. For example, if your program is a web application, its
interface could display a "Source" link that leads users to an archive
of the code. There are many ways you could offer source, and different
solutions
will be better for different programs; see section 13 for the
specific requirements.

You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU AGPL, see
<http://www.gnu.org/licenses/>.
`,
}
}
Copyright 2010 The Go Authors. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are
met:

* Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above
copyright notice, this list of conditions and the following disclaimer
in the documentation and/or other materials provided with the
distribution.
* Neither the name of Google Inc. nor the names of its
contributors may be used to endorse or promote products derived from
this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT

LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER
OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
Copyright 2014, Roger Peppe
All rights reserved.

Redistribution and use in source and binary forms, with or without modification,
are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright notice,
  this list of conditions and the following disclaimer in the documentation
  and/or other materials provided with the distribution.
* Neither the name of this project nor the names of its contributors
  may be used to endorse or promote products derived from this software
  without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT
SHALL THE COPYRIGHT
OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
Copyright (C) 2016 Trevor N. Suarez (Rican7)

Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the "Software"),
to deal in the Software without restriction, including without limitation
the rights to use, copy, modify, merge, publish, distribute, sublicense,
and/or sell copies of the Software, and to permit persons to whom the
Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included
in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES
OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.
IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM,
DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT,
TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION
WITH THE SOFTWARE
OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
The MIT License (MIT)

Copyright (c) 2016 Yasuhiro Matsumoto

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all
copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT
OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
SOFTWARE.
Copyright (C) 2012 Rob Figueiredo
All Rights Reserved.

MIT LICENSE

Permission is hereby granted, free of charge, to any person obtaining a copy of
this software and associated documentation files (the "Software"), to deal in
the Software without restriction, including without limitation the rights to
use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of
the Software, and to permit persons to whom the Software is furnished to do so,
subject to the following conditions:

The above copyright notice and this permission notice shall be included in all
copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS

FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN
CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
The MIT License (MIT)

Copyright (c) 2013 Armon Dadgar

Permission is hereby granted, free of charge, to any person obtaining a copy of
this software and associated documentation files (the "Software"), to deal in
the Software without restriction, including without limitation the rights to
use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of
the Software, and to permit persons to whom the Software is furnished to do so,
subject to the following conditions:

The above copyright notice and this permission notice shall be included in all
copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR
IN
CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
The MIT License

Copyright (c) 2014 Stretchr, Inc.
Copyright (c) 2017-2018 objx contributors

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all
copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT
OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE

```
SOFTWARE.
Paul Borman <borman@google.com>
bmatsuo
shawnps
theory
jboverfelt
dsymonds
cd1
wallclockbuilder
dansouza
// Copyright  2015 Steve Francia <spf@spf13.com>.
//
// Licensed under the Apache License, Version 2.0 (the "License");
// you may not use this file except in compliance with the License.
// You may obtain a copy of the License at
// http://www.apache.org/licenses/LICENSE-2.0
//
// Unless required by applicable law or agreed to in writing, software
// distributed under the License is distributed on an "AS IS" BASIS,
// WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
// See the License for the specific language governing permissions and
// limitations under the License.

// Parts inspired by https://github.com/ryanuber/go-license

package cmd

import (
 "strings"
 "time"

 "github.com/spf13/viper"
)

// Licenses contains all possible licenses a user can choose from.
var Licenses = make(map[string]License)

// License represents a software license agreement, containing the Name of
// the license, its possible matches (on the command line as given to cobra),
// the
 header to be used with each file on the file's creating, and the text
// of the license
type License struct {
 Name            string   // The type of license in use
 PossibleMatches []string // Similar names to guess
 Text            string   // License text data
 Header          string   // License header for source files
}
```

```
func init() {
 // Allows a user to not use a license.
 Licenses["none"] = License{"None", []string{"none", "false"}, "", ""}

 initApache2()
 initMit()
 initBsdClause3()
 initBsdClause2()
 initGpl2()
 initGpl3()
 initLgpl()
 initAgpl()
}

// getLicense returns license specified by user in flag or in config.
// If user didn't specify the license, it returns Apache License 2.0.
//
// TODO: Inspect project for existing license
func getLicense() License {
 // If explicitly flagged, use that.
 if userLicense != "" {
  return findLicense(userLicense)
 }

 // If user wants to have custom license, use that.
 if viper.IsSet("license.header") || viper.IsSet("license.text")
 {
  return License{Header: viper.GetString("license.header"),
   Text: viper.GetString("license.text")}
 }

 // If user wants to have built-in license, use that.
 if viper.IsSet("license") {
  return findLicense(viper.GetString("license"))
 }

 // If user didn't set any license, use Apache 2.0 by default.
 return Licenses["apache"]
}

func copyrightLine() string {
 author := viper.GetString("author")

 year := viper.GetString("year") // For tests.
 if year == "" {
  year = time.Now().Format("2006")
 }
```

```
 return "Copyright  " + year + " " + author
}

// findLicense looks for License object of built-in licenses.
// If it didn't find license, then the app will be terminated and
// error will be printed.
func findLicense(name string) License {
 found := matchLicense(name)
 if found == "" {
  er("unknown license: " + name)
 }
 return Licenses[found]
}

// matchLicense compares the given a license name
// to PossibleMatches of all built-in licenses.
// It returns blank string, if name is blank
 string or it didn't find
// then appropriate match to name.
func matchLicense(name string) string {
 if name == "" {
  return ""
 }

 for key, lic := range Licenses {
  for _, match := range lic.PossibleMatches {
   if strings.EqualFold(name, match) {
    return key
   }
  }
 }

 return ""
}
```

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by

the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but

excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this
License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute
copies of the
Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions

for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the

appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.

Copyright (c) 2013, The GoGo Authors. All rights reserved.

Protocol Buffers for Go with Gadgets

Go support for Protocol Buffers - Google's data interchange format

Copyright 2010 The Go Authors. All rights reserved.
https://github.com/golang/protobuf

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are
met:

* Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above
copyright notice, this list of conditions and the following disclaimer
in the documentation and/or other materials provided with the
distribution.
* Neither the name of Google Inc. nor the names of its
contributors may be used to endorse or promote products derived from
this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
"AS IS"
AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT
OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 2009,2014 Google Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are
met:

* Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above
copyright notice, this list of conditions and the following disclaimer
in the documentation and/or other materials provided with the
distribution.
* Neither the name of Google Inc. nor the names of its
contributors may be used to endorse or promote products derived from
this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT
OWNER
OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

1.57 nspr 4.12

1.57.1 Available under license :

Copyright 2005 Sun Microsystems, Inc. All rights reserved.
Use is subject to license terms.

This Source Code Form is subject to the terms of the Mozilla Public
License, v. 2.0. If a copy of the MPL was not distributed with this
file, You can obtain one at http://mozilla.org/MPL/2.0/.
Mozilla Public License Version 2.0
==================================

1. Definitions

1.1. "Contributor"
means each individual or legal entity that creates, contributes to
the creation of, or owns Covered Software.

1.2. "Contributor Version"
means the combination of the Contributions of others (if any) used
by a Contributor and that particular Contributor's Contribution.

1.3. "Contribution"
means Covered Software of a particular Contributor.

1.4. "Covered Software"
means Source Code Form to which the initial Contributor has attached the notice in Exhibit A, the Executable Form of such Source Code Form, and Modifications of such Source Code Form, in each case including portions thereof.

1.5. "Incompatible With Secondary Licenses"
means

(a) that the initial Contributor has attached the notice described in Exhibit B to the Covered Software; or

(b) that the Covered Software was made available under the terms of

version 1.1 or earlier of the License, but not also under the terms of a Secondary License.

1.6. "Executable Form"
means any form of the work other than Source Code Form.

1.7. "Larger Work"
means a work that combines Covered Software with other material, in a separate file or files, that is not Covered Software.

1.8. "License"
means this document.

1.9. "Licensable"
means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently, any and all of the rights conveyed by this License.

1.10. "Modifications"
means any of the following:

(a) any file in Source Code Form that results from an addition to, deletion from, or modification of the contents of Covered Software; or

(b) any new file in Source Code Form that contains any Covered Software.

1.11. "Patent Claims" of a Contributor
means any patent claim(s), including without limitation, method, process, and apparatus claims, in any patent Licensable by such Contributor that would be infringed, but for the grant of the License, by the making, using, selling, offering for sale, having made, import, or transfer of either its Contributions or its

Contributor Version.

1.12. "Secondary License"
means either the GNU General Public License, Version 2.0, the GNU Lesser General Public License, Version 2.1, the GNU Affero General Public License, Version 3.0, or any later versions of those licenses.

1.13. "Source Code Form"
means the form of the work preferred for making modifications.

1.14. "You" (or "Your")
means an individual or a legal entity exercising rights under this License. For legal entities, "You" includes any entity that controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. License Grants and Conditions

2.1. Grants

Each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license:

(a) under intellectual property rights (other than patent or trademark) Licensable by such Contributor to use, reproduce, make available, modify, display, perform, distribute, and otherwise exploit its Contributions, either on an unmodified basis, with Modifications, or as part of a Larger Work; and

(b) under Patent Claims of such Contributor to make, use, sell, offer for sale, have made, import, and otherwise transfer either its Contributions or its Contributor Version.

2.2. Effective Date

The licenses granted in Section 2.1 with respect to any Contribution become effective for each Contribution on the date the Contributor first distributes
such Contribution.

2.3. Limitations on Grant Scope

The licenses granted in this Section 2 are the only rights granted under this License. No additional rights or licenses will be implied from the distribution or licensing of Covered Software under this License. Notwithstanding Section 2.1(b) above, no patent license is granted by a Contributor:

(a) for any code that a Contributor has removed from Covered Software; or

(b) for infringements caused by: (i) Your and any other third party's modifications of Covered Software, or (ii) the combination of its Contributions with other software (except as part of its Contributor Version); or

(c) under Patent Claims infringed by Covered Software in the absence of its Contributions.

This License does not grant any rights in the trademarks, service marks, or logos of any Contributor (except as may be necessary to comply with the notice requirements in Section 3.4).

2.4. Subsequent Licenses

No Contributor makes
additional grants as a result of Your choice to
distribute the Covered Software under a subsequent version of this License (see Section 10.2) or under the terms of a Secondary License (if permitted under the terms of Section 3.3).

2.5. Representation

Each Contributor represents that the Contributor believes its Contributions are its original creation(s) or it has sufficient rights to grant the rights to its Contributions conveyed by this License.

2.6. Fair Use

This License is not intended to limit any rights You have under applicable copyright doctrines of fair use, fair dealing, or other equivalents.

2.7. Conditions

Sections 3.1, 3.2, 3.3, and 3.4 are conditions of the licenses granted in Section 2.1.

3. Responsibilities

3.1. Distribution of Source Form

All distribution of Covered Software in Source Code Form, including any Modifications that You create or to which You contribute, must be under the terms of this License. You must inform recipients that the Source Code Form of the Covered Software is governed by the terms of this License, and how they can obtain a copy of this License. You may not attempt to alter or restrict the recipients' rights in the Source Code Form.

3.2. Distribution of Executable Form

If You distribute Covered Software in Executable Form then:

(a) such Covered Software must also be made available in Source Code Form, as described in Section 3.1, and You must inform recipients of the Executable Form how they can obtain a copy of such Source Code Form by reasonable means in a timely manner, at a charge no more than the cost of distribution to the recipient; and

(b) You may distribute such Executable Form under the terms of this License, or sublicense it under different terms, provided that the license for the Executable Form does not attempt to limit or alter the recipients' rights in the Source Code Form under this License.

3.3. Distribution of a Larger Work

You may create and distribute a Larger Work under terms of Your choice, provided that You also comply with the requirements of this License for the Covered Software. If the Larger Work is a combination of Covered Software with a work governed by one or more Secondary Licenses, and the Covered Software is not Incompatible With Secondary Licenses, this License permits You to additionally distribute such Covered Software under the terms of such Secondary License(s), so that the recipient of the Larger Work may, at their option, further distribute the Covered Software under the terms of either this License or such Secondary License(s).

3.4. Notices

You may not remove or alter the substance of any license notices (including copyright notices, patent notices, disclaimers of warranty, or limitations of liability) contained within the Source Code Form of the Covered Software, except that You may alter any license notices to the extent required to remedy known factual inaccuracies.

3.5. Application of Additional
Terms

You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Software. However, You may do so only on Your own behalf, and not on behalf of any Contributor. You must make it absolutely clear that any such warranty, support, indemnity, or liability obligation is offered by You alone, and You hereby agree to indemnify every Contributor for any liability incurred by such Contributor as a result of warranty, support, indemnity or liability terms You offer. You may include additional disclaimers of warranty and limitations of liability specific to any jurisdiction.

4. Inability to Comply Due to Statute or Regulation

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Software due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the
maximum extent possible; and (b)
describe the limitations and the code they affect. Such description must be placed in a text file included with all distributions of the Covered Software under this License. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Termination

5.1. The rights granted under this License will terminate automatically if You fail to comply with any of its terms. However, if You become compliant, then the rights granted under this License from a particular Contributor are reinstated (a) provisionally, unless and until such Contributor explicitly and finally terminates Your grants, and (b) on an ongoing basis, if such Contributor fails to notify You of the non-compliance by some reasonable means prior to 60 days after You have come back into compliance. Moreover, Your grants from a particular Contributor are reinstated on an ongoing
basis if such Contributor
notifies You of the non-compliance by some reasonable means, this is the first time You have received notice of non-compliance with this License from such Contributor, and You become compliant prior to 30 days after Your receipt of the notice.

5.2. If You initiate litigation against any entity by asserting a patent

infringement claim (excluding declaratory judgment actions,
counter-claims, and cross-claims) alleging that a Contributor Version
directly or indirectly infringes any patent, then the rights granted to
You by any and all Contributors for the Covered Software under Section
2.1 of this License shall terminate.

5.3. In the event of termination under Sections 5.1 or 5.2 above, all
end user license agreements (excluding distributors and resellers) which
have been validly granted by You or Your distributors under this License
prior to termination shall survive termination.

```
************************************************************************
*                                                                      *
*  6. Disclaimer of Warranty                                           *
*  -------------------------                                           *
*                                                                      *
*  Covered Software is provided under this License on an "as is"       *
*  basis, without warranty of any kind, either expressed, implied, or  *
*  statutory, including, without limitation, warranties that the       *
*  Covered Software is free of defects, merchantable, fit for a        *
*  particular purpose or non-infringing. The entire risk as to the     *
*  quality and performance of the Covered Software is with You.        *
*  Should any Covered Software prove defective in any respect, You     *
*  (not any Contributor) assume the cost of any necessary servicing,   *
*  repair, or correction. This disclaimer of warranty constitutes an   *
*  essential part of this License. No use of any Covered
 Software is   *
*  authorized under this License except under this disclaimer.         *
*                                                                      *
************************************************************************

************************************************************************
*                                                                      *
*  7. Limitation of Liability                                          *
*  --------------------------                                          *
*                                                                      *
*  Under no circumstances and under no legal theory, whether tort      *
*  (including negligence), contract, or otherwise, shall any           *
*  Contributor, or anyone who distributes Covered Software as          *
*  permitted above, be liable to You for any direct, indirect,         *
*  special, incidental, or consequential damages of any character      *
*  including, without limitation,
 damages for lost profits, loss of    *
*  goodwill, work stoppage, computer failure or malfunction, or any    *
*  and all other commercial damages or losses, even if such party      *
*  shall have been informed of the possibility of such damages. This   *
*  limitation of liability shall not apply to liability for death or   *
```

* personal injury resulting from such party's negligence to the *
* extent applicable law prohibits such limitation. Some *
* jurisdictions do not allow the exclusion or limitation of *
* incidental or consequential damages, so this exclusion and *
* limitation may not apply to You. *
* *
****

8. Litigation

Any litigation relating to this License may be brought only in the courts of a jurisdiction where the defendant maintains its principal place
of business and such litigation shall be governed by laws of that jurisdiction, without reference to its conflict-of-law provisions. Nothing in this Section shall prevent a party's ability to bring cross-claims or counter-claims.

9. Miscellaneous

This License represents the complete agreement concerning the subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not be used to construe this License against a Contributor.

10. Versions of the License

10.1. New Versions

Mozilla Foundation is the license steward. Except as provided in Section 10.3, no one other than the license steward has the right to modify or publish new versions of this License. Each version will be given a distinguishing version
number.

10.2. Effect of New Versions

You may distribute the Covered Software under the terms of the version of the License under which You originally received the Covered Software, or under the terms of any subsequent version published by the license steward.

10.3. Modified Versions

If you create software not governed by this License, and you want to create a new license for such software, you may create and use a modified version of this License if you rename the license and remove any references to the name of the license steward (except to note that such modified license differs from this License).

10.4. Distributing Source Code Form that is Incompatible With Secondary Licenses

If You choose to distribute Source Code Form that is Incompatible With Secondary Licenses under the terms of this version of the License, the notice described in Exhibit B of this License must be attached.

Exhibit A - Source Code Form License Notice

This Source Code Form is subject to the terms of the Mozilla Public License, v. 2.0. If a copy of the MPL was not distributed with this file, You can obtain one at http://mozilla.org/MPL/2.0/.

If it is not possible or desirable to put the notice in a particular file, then You may include the notice in a location (such as a LICENSE file in a relevant directory) where a recipient would be likely to look for such a notice.

You may add additional accurate notices of copyright ownership.

Exhibit B - "Incompatible With Secondary Licenses" Notice

This Source Code Form is "Incompatible With Secondary Licenses", as defined by the Mozilla Public License, v. 2.0.

1.58 wget 1.18

1.58.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <https://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for
software and other kinds of works.

The licenses for most software and other practical works are designed
to take away your freedom to share and change the works. By contrast,
the GNU General Public License is intended to guarantee your freedom to
share and change all versions of a program--to make sure it remains free
software for all its users. We, the Free Software Foundation, use the
GNU General Public License for most of our software; it applies also to
any other work released this way by its authors. You can apply it to
your programs, too.

When we speak of free software, we are referring to
freedom, not
price. Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
them if you wish), that you receive source code or can get it if you
want it, that you can change the software or use pieces of it in new
free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you
these rights or asking you to surrender the rights. Therefore, you have
certain responsibilities if you distribute copies of the software, or if
you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether
gratis or for a fee, you must pass on to the recipients the same
freedoms that you received. You must make sure that they, too, receive
or can get the source code. And you must show them these terms so they
know their rights.

Developers that use the GNU GPL protect your rights with two steps:
(1)
assert copyright on the software, and (2) offer you this License
giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains
that there is no warranty for this free software. For both users' and
authors' sake, the GPL requires that modified versions be marked as
changed, so that their problems will not be attributed erroneously to
authors of previous versions.

Some devices are designed to deny users access to install or run
modified versions of the software inside them, although the manufacturer
can do so. This is fundamentally incompatible with the aim of
protecting users' freedom to change the software. The systematic
pattern of such abuse occurs in the area of products for individuals to
use, which is precisely where it is most unacceptable. Therefore, we

have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand
ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees"
and
"recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy,

is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is
covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed;
section 10
makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of

technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately
publish on each copy an appropriate copyright notice;
keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to
"keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution

medium, is called an
"aggregate" if the compilation and its resulting copyright are not
used to limit the access or legal rights of the compilation's users
beyond what the individual works permit. Inclusion of a covered work
in an aggregate does not cause this License to apply to the other
parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms
of sections 4 and 5, provided that you also convey the
machine-readable Corresponding Source under the terms of this License,
in one of these ways:

a) Convey the object code in, or embodied in, a physical product
(including a physical distribution medium), accompanied by the
Corresponding Source fixed on a durable physical medium
customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product
(including a physical distribution medium), accompanied by a
written offer, valid for at least three years
and valid for as
long as you offer spare parts or customer support for that product
model, to give anyone who possesses the object code either (1) a
copy of the Corresponding Source for all the software in the
product that is covered by this License, on a durable physical
medium customarily used for software interchange, for a price no
more than your reasonable cost of physically performing this
conveying of source, or (2) access to copy the
Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the
written offer to provide the Corresponding Source. This
alternative is allowed only occasionally and noncommercially, and
only if you received the object code with such an offer, in accord
with subsection 6b.

d) Convey the object code by offering access from a designated
place (gratis or for a charge), and offer equivalent access to the
Corresponding Source in
the same way through the same place at no
further charge. You need not require recipients to copy the
Corresponding Source along with the object code. If the place to
copy the object code is a network server, the Corresponding Source
may be on a different server (operated by you or a third party)
that supports equivalent copying facilities, provided you maintain
clear directions next to the object code saying where to find the

Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on

those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above
requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright
holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights
granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation

(including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this

License will continue to apply to the part which is the covered work,
but the special requirements of the GNU Affero General Public License,
section 13, concerning interaction through a network will apply to the
combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of
the GNU General Public License from time to time. Such new versions will
be similar in spirit to the present version, but may differ in detail to
address new problems or concerns.

Each version is given a distinguishing version number. If the
Program specifies that a certain numbered version of the GNU General
Public License "or any later version" applies to it, you
have the
option of following the terms and conditions either of that numbered
version or of any later version published by the Free Software
Foundation. If the Program does not specify a version number of the
GNU General Public License, you may choose any version ever published
by the Free Software Foundation.

If the Program specifies that a proxy can decide which future
versions of the GNU General Public License can be used, that proxy's
public statement of acceptance of a version permanently authorizes you
to choose that version for the Program.

Later license versions may give you additional or different
permissions. However, no additional obligations are imposed on any
author or copyright holder as a result of your choosing to follow a
later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY
APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT
HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS"
WITHOUT WARRANTY
OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM
IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF
ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING
WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS

THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17.
Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see <https://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>
This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<https://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what you want
to do, use the GNU Lesser General
Public License instead of this License. But first, please read
<https://www.gnu.org/philosophy/why-not-lgpl.html>.

1.59 sudo 1.8.17

1.59.1 Available under license :

Permission to use, copy, modify, and/or distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

1.60 tcl 8.6.6

1.60.1 Available under license :

The author disclaims copyright to this source code. In place of
a legal notice, here is a blessing:

   May you do good and not evil.
   May you find forgiveness for yourself and forgive others.
   May you share freely, never taking more than you give.
This is a mostly rewritten version of [incr Tcl], which is copyrighted
by Arnulf P. Wiedemann (c) Copyright 2008. It is derived from a version
written by Lucent Technologies, Inc., and other parties see that copyright
below.

The rewritten version is copyrighted with BSD license or Public Domain at
your choice.

The original version of this software is copyrighted by Lucent Technologies,
Inc., and other parties. The following terms apply to all files associated
with the software unless explicitly disclaimed in individual files.

The authors hereby grant permission to use, copy, modify, distribute,
and license this software and its documentation for any purpose, provided
that existing copyright notices are retained in all copies and that this
notice is included verbatim in any distributions. No written agreement,
license, or royalty fee is required for any of the authorized uses.
Modifications to this software may be copyrighted by their authors
and need not follow the licensing terms described
 here, provided that
the new terms are clearly indicated on the first page of each file where
they apply.

IN NO EVENT SHALL THE AUTHORS OR DISTRIBUTORS BE LIABLE TO ANY PARTY
FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES
ARISING OUT OF THE USE OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY
DERIVATIVES THEREOF, EVEN IF THE AUTHORS HAVE BEEN ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

THE AUTHORS AND DISTRIBUTORS SPECIFICALLY DISCLAIM ANY WARRANTIES,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THIS SOFTWARE
IS PROVIDED ON AN "AS IS" BASIS, AND THE AUTHORS AND DISTRIBUTORS HAVE
NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR

MODIFICATIONS.

GOVERNMENT USE: If you are acquiring this software on behalf of the
U.S. government, the Government shall have only "Restricted Rights"
in the software and related documentation as defined in the Federal
Acquisition
Regulations (FARs) in Clause 52.227.19 (c) (2). If you
are acquiring the software on behalf of the Department of Defense, the
software shall be classified as "Commercial Computer Software" and the
Government shall have only "Restricted Rights" as defined in Clause
252.227-7013 (c) (1) of DFARs. Notwithstanding the foregoing, the
authors grant the U.S. Government and others acting in its behalf
permission to use and distribute the software in accordance with the
terms specified in this license.
This software is copyrighted by Kevin B. Kenny, and by other parties.
The following terms apply to all files associated with the software
unless explicitly disclaimed in individual files.

The authors hereby grant permission to use, copy, modify, distribute,
and license this software and its documentation for any purpose, provided
that existing copyright notices are retained in all copies and that this
notice is included verbatim in any distributions. No written agreement,
license, or royalty fee is required for any of the authorized uses.
Modifications to this software may be copyrighted by their authors
and need not follow the licensing terms described here, provided that
the new terms are clearly indicated on the first page of each file where
they apply.

IN NO EVENT SHALL THE AUTHORS OR DISTRIBUTORS BE LIABLE TO ANY PARTY
FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES
ARISING OUT OF THE USE OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY
DERIVATIVES THEREOF, EVEN IF
THE AUTHORS HAVE BEEN ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

THE AUTHORS AND DISTRIBUTORS SPECIFICALLY DISCLAIM ANY WARRANTIES,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THIS SOFTWARE
IS PROVIDED ON AN "AS IS" BASIS, AND THE AUTHORS AND DISTRIBUTORS HAVE
NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR
MODIFICATIONS.

GOVERNMENT USE: If you are acquiring this software on behalf of the
U.S. government, the Government shall have only "Restricted Rights"
in the software and related documentation as defined in the Federal
Acquisition Regulations (FARs) in Clause 52.227.19 (c) (2). If you
are acquiring the software on behalf of the Department of Defense, the
software shall be classified as "Commercial Computer Software" and the

Government shall have only "Restricted Rights" as defined in Clause
252.227-7013 (c) (1) of DFARs. Notwithstanding the foregoing, the
authors grant
 the U.S. Government and others acting in its behalf
permission to use and distribute the software in accordance with the
terms specified in this license.

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>> [incr Tcl] <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

AUTHOR: Michael J. McLennan
        Bell Labs Innovations for Lucent Technologies
        mmclennan@lucent.com
        http://www.tcltk.com/itcl
==========
          Copyright (c) 1993-1996 Lucent Technologies
==========
Permission to use, copy, modify, and distribute this software and its
documentation for any purpose and without fee is hereby granted,
provided that the above copyright notice appear in all copies and that
both that the copyright notice and warranty disclaimer appear in
supporting documentation, and that the names of Lucent Technologies
any of their entities not be used in advertising or publicity
pertaining to distribution of the software without specific, written
prior permission.

Lucent Technologies
 disclaims all warranties with regard to this
software, including all implied warranties of merchantability and
fitness. In no event shall Lucent be liable for any special, indirect
or consequential damages or any damages whatsoever resulting from loss
of use, data or profits, whether in an action of contract, negligence
or other tortuous action, arising out of or in connection with the use
or performance of this software.
==========
This software is copyrighted by Slawomir Cygan, and by other parties.
The following terms apply to all files associated with the software
unless explicitly disclaimed in individual files.

The authors hereby grant permission to use, copy, modify, distribute,
and license this software and its documentation for any purpose, provided
that existing copyright notices are retained in all copies and that this
notice is included verbatim in any distributions. No written agreement,
license, or royalty fee is required for any of the authorized uses.
Modifications to this software may be copyrighted by their authors
and need not follow the licensing terms described here, provided that
the new terms are clearly indicated on the first page of each file where
they apply.

IN NO EVENT SHALL THE AUTHORS OR DISTRIBUTORS BE LIABLE TO ANY PARTY
FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES
ARISING OUT OF THE USE OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY
DERIVATIVES THEREOF, EVEN IF
THE AUTHORS HAVE BEEN ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

THE AUTHORS AND DISTRIBUTORS SPECIFICALLY DISCLAIM ANY WARRANTIES,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THIS SOFTWARE
IS PROVIDED ON AN "AS IS" BASIS, AND THE AUTHORS AND DISTRIBUTORS HAVE
NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR
MODIFICATIONS.

GOVERNMENT USE: If you are acquiring this software on behalf of the
U.S. government, the Government shall have only "Restricted Rights"
in the software and related documentation as defined in the Federal
Acquisition Regulations (FARs) in Clause 52.227.19 (c) (2). If you
are acquiring the software on behalf of the Department of Defense, the
software shall be classified as "Commercial Computer Software" and the
Government shall have only "Restricted Rights" as defined in Clause
252.227-7013 (c) (1) of DFARs. Notwithstanding the foregoing, the
authors grant
the U.S. Government and others acting in its behalf
permission to use and distribute the software in accordance with the
terms specified in this license.
This software is copyrighted by Kevin B. Kenny, and by other parties.
The following terms apply to all files associated with the software
unless explicitly disclaimed in individual files.

The authors hereby grant permission to use, copy, modify, distribute,
and license this software and its documentation for any purpose, provided
that existing copyright notices are retained in all copies and that this
notice is included verbatim in any distributions. No written agreement,
license, or royalty fee is required for any of the authorized uses.
Modifications to this software may be copyrighted by their authors
and need not follow the licensing terms described here, provided that
the new terms are clearly indicated on the first page of each file where
they apply.

IN NO EVENT SHALL THE AUTHORS OR DISTRIBUTORS BE LIABLE TO ANY PARTY
FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES
ARISING OUT OF THE USE OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY
DERIVATIVES THEREOF, EVEN IF
THE AUTHORS HAVE BEEN ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

THE AUTHORS AND DISTRIBUTORS SPECIFICALLY DISCLAIM ANY WARRANTIES,

INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THIS SOFTWARE IS PROVIDED ON AN "AS IS" BASIS, AND THE AUTHORS AND DISTRIBUTORS HAVE NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

GOVERNMENT USE: If you are acquiring this software on behalf of the U.S. government, the Government shall have only "Restricted Rights" in the software and related documentation as defined in the Federal Acquisition Regulations (FARs) in Clause 52.227.19 (c) (2). If you are acquiring the software on behalf of the Department of Defense, the software shall be classified as "Commercial Computer Software" and the Government shall have only "Restricted Rights" as defined in Clause 252.227-7013 (c) (1) of DFARs. Notwithstanding the foregoing, the authors grant
the U.S. Government and others acting in its behalf
permission to use and distribute the software in accordance with the terms specified in this license.
This software is copyrighted by the Regents of the University of California, Sun Microsystems, Inc., Scriptics Corporation, and other parties. The following terms apply to all files associated with the software unless explicitly disclaimed in individual files.

The authors hereby grant permission to use, copy, modify, distribute, and license this software and its documentation for any purpose, provided that existing copyright notices are retained in all copies and that this notice is included verbatim in any distributions. No written agreement, license, or royalty fee is required for any of the authorized uses. Modifications to this software may be copyrighted by their authors and need not follow the licensing terms described here, provided that the new terms are clearly indicated on the first page of each file where they apply.

IN NO EVENT SHALL THE AUTHORS OR DISTRIBUTORS BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE
OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY DERIVATIVES THEREOF, EVEN IF THE AUTHORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE AUTHORS AND DISTRIBUTORS SPECIFICALLY DISCLAIM ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THIS SOFTWARE IS PROVIDED ON AN "AS IS" BASIS, AND THE AUTHORS AND DISTRIBUTORS HAVE NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

GOVERNMENT USE: If you are acquiring this software on behalf of the

U.S. government, the Government shall have only "Restricted Rights"
in the software and related documentation as defined in the Federal
Acquisition Regulations (FARs) in Clause 52.227.19 (c) (2). If you
are acquiring the software on behalf of the Department of Defense, the
software shall be classified as "Commercial Computer Software" and the
Government shall have only "Restricted Rights" as defined in Clause
252.227-7013
(c) (1) of DFARs. Notwithstanding the foregoing, the
authors grant the U.S. Government and others acting in its behalf
permission to use and distribute the software in accordance with the
terms specified in this license.
Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization
obtaining a copy of the software and accompanying documentation covered by
this license (the "Software") to use, reproduce, display, distribute,
execute, and transmit the Software, and to prepare derivative works of the
Software, and to permit third-parties to whom the Software is furnished to
do so, all subject to the following:

The copyright notices in the Software and this entire statement, including
the above license grant, this restriction and the following disclaimer,
must be included in all copies of the Software, in whole or in part, and
all derivative works of the Software, unless such copies or derivative
works are solely in the form of machine-executable object code generated by
a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES
OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT
SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE
FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE,
ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER
DEALINGS IN THE SOFTWARE.
This software is copyrighted by the Regents of the University of
California, Sun Microsystems, Inc., Scriptics Corporation, ActiveState
Corporation and other parties. The following terms apply to all files
associated with the software unless explicitly disclaimed in
individual files.

The authors hereby grant permission to use, copy, modify, distribute,
and license this software and its documentation for any purpose, provided
that existing copyright notices are retained in all copies and that this
notice is included verbatim in any distributions. No written agreement,
license, or royalty fee is required for any of the authorized uses.
Modifications to this software may be copyrighted by their authors
and need not follow the licensing terms described here, provided that

the new terms are clearly indicated on the first page of each file where
they apply.

IN NO EVENT SHALL THE AUTHORS OR DISTRIBUTORS BE LIABLE TO ANY PARTY
FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES
ARISING
OUT OF THE USE OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY
DERIVATIVES THEREOF, EVEN IF THE AUTHORS HAVE BEEN ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

THE AUTHORS AND DISTRIBUTORS SPECIFICALLY DISCLAIM ANY WARRANTIES,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THIS SOFTWARE
IS PROVIDED ON AN "AS IS" BASIS, AND THE AUTHORS AND DISTRIBUTORS HAVE
NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR
MODIFICATIONS.

GOVERNMENT USE: If you are acquiring this software on behalf of the
U.S. government, the Government shall have only "Restricted Rights"
in the software and related documentation as defined in the Federal
Acquisition Regulations (FARs) in Clause 52.227.19 (c) (2). If you
are acquiring the software on behalf of the Department of Defense, the
software shall be classified as "Commercial Computer Software" and the
Government shall have only "Restricted Rights" as
defined in Clause
252.227-7014 (b) (3) of DFARs. Notwithstanding the foregoing, the
authors grant the U.S. Government and others acting in its behalf
permission to use and distribute the software in accordance with the
terms specified in this license.
This software is copyrighted by the Scriptics Corporation, and other
parties. The following terms apply to all files associated with the
software unless explicitly disclaimed in individual files.

The authors hereby grant permission to use, copy, modify, distribute,
and license this software and its documentation for any purpose, provided
that existing copyright notices are retained in all copies and that this
notice is included verbatim in any distributions. No written agreement,
license, or royalty fee is required for any of the authorized uses.
Modifications to this software may be copyrighted by their authors
and need not follow the licensing terms described here, provided that
the new terms are clearly indicated on the first page of each file where
they apply.

IN NO EVENT SHALL THE AUTHORS OR DISTRIBUTORS BE LIABLE TO ANY PARTY
FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES
ARISING OUT OF THE USE OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY
DERIVATIVES THEREOF,

EVEN IF THE AUTHORS HAVE BEEN ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

THE AUTHORS AND DISTRIBUTORS SPECIFICALLY DISCLAIM ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THIS SOFTWARE IS PROVIDED ON AN "AS IS" BASIS, AND THE AUTHORS AND DISTRIBUTORS HAVE NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

GOVERNMENT USE: If you are acquiring this software on behalf of the U.S. government, the Government shall have only "Restricted Rights" in the software and related documentation as defined in the Federal Acquisition Regulations (FARs) in Clause 52.227.19 (c) (2). If you are acquiring the software on behalf of the Department of Defense, the software shall be classified as "Commercial Computer Software" and the Government shall have only "Restricted Rights" as defined in Clause 252.227-7013 (c) (1) of DFARs. Notwithstanding the foregoing, the authors
grant the U.S. Government and others acting in its behalf
permission to use and distribute the software in accordance with the terms specified in this license.

1.61 gpgme 1.10.0

1.61.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not

price. Our General Public Licenses are designed
to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid
anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate to certain responsibilities for you if you
distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether
gratis or for a fee, you must give the recipients all the rights that
you have. You must make sure that they, too, receive or can get the
source code. And you must show them these terms so they know their
rights.

We protect your rights with two steps: (1) copyright the software, and
(2) offer you this license which gives you legal permission to copy,
distribute
and/or modify the software.

Also, for each author's protection and ours, we want to make certain
that everyone understands that there is no warranty for this free
software. If the software is modified by someone else and passed on, we
want its recipients to know that what they have is not the original, so
that any problems introduced by others will not reflect on the original
authors' reputations.

Finally, any free program is threatened constantly by software
patents. We wish to avoid the danger that redistributors of a free
program will individually obtain patent licenses, in effect making the
program proprietary. To prevent this, we have made it clear that any
patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and
modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which
contains
a notice placed by the copyright holder saying it may be distributed
under the terms of this General Public License. The "Program", below,
refers to any such program or work, and a "work based on the Program"
means either the Program or any derivative work under copyright law:

that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any

associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the
source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each
time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you

may not distribute the Program at all. For example, if a patent
license would not permit royalty-free redistribution
of the Program by
all those who receive copies directly or indirectly through you, then
the only way you could satisfy both it and this License would be to
refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under
any particular circumstance, the balance of the section is intended to
apply and the section as a whole is intended to apply in other
circumstances.

It is not the purpose of this section to induce you to infringe any
patents or other property right claims or to contest validity of any
such claims; this section has the sole purpose of protecting the
integrity of the free software distribution system, which is
implemented by public license practices. Many people have made
generous contributions to the wide range of software distributed
through that system in reliance on consistent application of that
system; it is up to the author/donor to decide if he or she is willing
to distribute software through
any other system and a licensee cannot
impose that choice.

This section is intended to make thoroughly clear what is believed to
be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in
certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Program under this License
may add an explicit geographical distribution limitation excluding
those countries, so that distribution is permitted only in or among
countries not thus excluded. In such case, this License incorporates
the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions
of the General Public License from time to time. Such new versions will
be similar in spirit to the present version, but may differ in detail to
address new problems or concerns.

Each version is given a distinguishing version number. If the Program
specifies a version number
of this License which applies to it and "any
later version", you have the option of following the terms and conditions
either of that version or of any later version published by the Free
Software Foundation. If the Program does not specify a version number of
this License, you may choose any version ever published by the Free Software
Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW.
EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN
IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation; either version 2 of the License,
or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and
`show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this is what you want to do, use the GNU Library General
Public License instead of this License.

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them

with the library after making changes to the library and recompiling
it. And you must show them these terms so they know their rights.

 We protect your rights with a two-step method: (1) we copyright the
library, and (2) we offer you this license, which gives you legal
permission to copy, distribute and/or modify the library.

 To protect each distributor, we want to make it very clear that
there is no warranty for the free library. Also, if the library is
modified by someone else and passed on, the recipients should know
that what they have is not the original version, so that the original
author's reputation will not be affected by problems that might be
introduced by others.
^L
 Finally, software
 patents pose a constant threat to the existence of
any free program. We wish to make sure that a company cannot
effectively restrict the users of a free program by obtaining a
restrictive license from a patent holder. Therefore, we insist that
any patent license obtained for a version of the library must be
consistent with the full freedom of use specified in this license.

 Most GNU software, including some libraries, is covered by the
ordinary GNU General Public License. This license, the GNU Lesser
General Public License, applies to certain designated libraries, and
is quite different from the ordinary General Public License. We use
this license for certain libraries in order to permit linking those
libraries into non-free programs.

 When a program is linked with a library, whether statically or using
a shared library, the combination of the two is legally speaking a
combined work, a derivative of the original library. The ordinary
General Public License therefore permits
 such linking only if the
entire combination fits its criteria of freedom. The Lesser General
Public License permits more lax criteria for linking other code with
the library.

 We call this license the "Lesser" General Public License because it
does Less to protect the user's freedom than the ordinary General
Public License. It also provides other free software developers Less
of an advantage over competing non-free programs. These disadvantages
are the reason we use the ordinary General Public License for many
libraries. However, the Lesser license provides advantages in certain
special circumstances.

 For example, on rare occasions, there may be a special need to
encourage the widest possible use of a certain library, so that it

becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting
the free library to free
software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order
to run.
^L

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into
another language. (Hereinafter, translation is
included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can
be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the
ordinary GNU General Public
License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.
^L
Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or

derivative of it, under Section 2) in object code or executable form
under the terms of Sections 1 and 2 above provided that you accompany
it with the complete
corresponding machine-readable source code, which
must be distributed under the terms of Sections 1 and 2 above on a
medium customarily used for software interchange.

If distribution of object code is made by offering access to copy
from a designated place, then offering equivalent access to copy the
source code from the same place satisfies the requirement to
distribute the source code, even though third parties are not
compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the
Library, but is designed to work with the Library by being compiled or
linked with it, is called a "work that uses the Library". Such a
work, in isolation, is not a derivative work of the Library, and
therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library
creates an executable that is a derivative of the Library (because it
contains portions of the Library), rather than a "work
that uses the
library". The executable is therefore covered by this License.
Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file
that is part of the Library, the object code for the work may be a
derivative work of the Library even though the source code is not.
Whether this is true is especially significant if the work can be
linked without the Library, or if the work is itself a library. The
threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data
structure layouts and accessors, and small macros and small inline
functions (ten lines or less in length), then the use of the object
file is unrestricted, regardless of whether it is legally a derivative
work. (Executables containing this object code plus portions of the
Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may
distribute
the object code for the work under the terms of Section 6.
Any executables containing that work also fall under Section 6,
whether or not they are linked directly with the Library itself.
^L
6. As an exception to the Sections above, you may also combine or
link a "work that uses the Library" with the Library to produce a

work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a)
Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will
operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the

Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is
normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.
^L
7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined
with any other library
facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited
by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying

the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.
^L
11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they
do not
excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution
system which is
implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those

countries, so that distribution is permitted only in or among
countries not thus excluded. In such case, this License incorporates
the limitation as if written in the body of this License.

13. The Free Software Foundation
may publish revised and/or new
versions of the Lesser General Public License from time to time.
Such new versions will be similar in spirit to the present version,
but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library
specifies a version number of this License which applies to it and
"any later version", you have the option of following the terms and
conditions either of that version or of any later version published by
the Free Software Foundation. If the Library does not specify a
license version number, you may choose any version ever published by
the Free Software Foundation.
^L
14. If you wish to incorporate parts of the Library into other free
programs whose distribution conditions are incompatible with these,
write to the author to ask for permission. For software which is
copyrighted by the Free Software Foundation, write to the Free
Software Foundation; we sometimes make exceptions for this.
Our
decision will be guided by the two goals of preserving the free status
of all derivatives of our free software and of promoting the sharing
and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO
WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW.
EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR
OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY
KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE
LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME
THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN
WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY
AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED
ABOVE, BE LIABLE TO YOU
FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR
CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE
LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING
RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A

FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

^L

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James

Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

1.62 lvm2 2.02.166

1.62.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it. (Some other Free Software Foundation software is covered by
the GNU Lesser General Public License instead.)
You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price. Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid
anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate to certain responsibilities for you if you
distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether
gratis or for a fee, you must give the recipients
all the rights that
you have. You must make sure that they, too, receive or can get the

source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate

copyright notice and disclaimer of warranty;
keep intact all the
notices that refer to this License and to the absence of any warranty;
and give any other recipients of the Program a copy of this License
along with the Program.

You may charge a fee for the physical act of transferring a copy, and
you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion
of it, thus forming a work based on the Program, and copy and
distribute such modifications or work under the terms of Section 1
above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices
stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in
whole or in part contains or is
derived from the Program or any
part thereof, to be licensed as a whole at no charge to all third
parties under the terms of this License.

c) If the modified program normally reads commands interactively
when run, you must cause it, when started running for such
interactive use in the most ordinary way, to print or display an
announcement including an appropriate copyright notice and a
notice that there is no warranty (or else, saying that you provide
a warranty) and that users may redistribute the program under
these conditions, and telling the user how to view a copy of this
License. (Exception: if the Program itself is interactive but
does not normally print such an announcement, your work based on
the Program is not required to print an announcement.)

These requirements apply to the modified
work as a whole. If
identifiable sections of that work are not derived from the Program,
and can be reasonably considered independent and separate works in
themselves, then this License, and its terms, do not apply to those
sections when you distribute them as separate works. But when you
distribute the same sections as part of a whole which is a work based
on the Program, the distribution of the whole must be on the terms of
this License, whose permissions for other licensees extend to the
entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest
your rights to work written entirely by you; rather, the intent is to
exercise the right to control the distribution of derivative or

collective works based on the Program.

In addition, mere aggregation
of another work not based on the Program
with the Program (or with a work based on the Program) on a volume of
a storage or distribution medium does not bring the other work under
the scope of this License.

3. You may copy and distribute the Program (or a work based on it,
under Section 2) in object code or executable form under the terms of
Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable
source code, which must be distributed under the terms of Sections
1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three
years, to give any third party, for a charge no more than your
cost of physically performing source distribution, a complete

machine-readable copy of the corresponding source code, to be
distributed under the terms of Sections 1 and 2 above on a medium
customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer
to distribute corresponding source code. (This alternative is
allowed only for noncommercial distribution and only if you
received the program in object code or executable form with such
an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for
making modifications to it. For an executable work, complete source
code means all the source code for all modules it contains, plus any
associated interface definition files, plus the scripts used to
control compilation and installation of the executable. However, as a

special exception, the source code distributed need not include
anything that is normally distributed (in either source or binary
form) with the major components (compiler, kernel, and so on) of the
operating system on which the executable runs, unless that component
itself accompanies the executable.

If distribution of executable or object code is made by offering
access to copy from a designated place, then offering equivalent
access to copy the source code from the same place counts as
distribution of the source code, even though third parties are not
compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate
your rights under this License.
However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license
from the
original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent
license
would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any

such claims; this section has the sole purpose of protecting the
integrity of the free software distribution system, which is
implemented by public license practices. Many people have made
generous contributions to the wide range of software
distributed
through that system in reliance on consistent application of that
system; it is up to the author/donor to decide if he or she is willing
to distribute software through any other system and a licensee cannot
impose that choice.

This section is intended to make thoroughly clear what is believed to
be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in
certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Program under this License
may add an explicit geographical distribution limitation excluding
those countries, so that distribution is permitted only in or among
countries not thus excluded. In such case, this License incorporates
the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions
of the General Public License from time to time. Such new versions will
be similar in spirit to the present version, but may differ in detail to
address new problems or concerns.

Each version is given a distinguishing version number. If the Program
specifies a version number of this License which applies to it and "any
later version", you have the option of following the terms and conditions
either of that version or of any later version published by the Free
Software Foundation. If the Program does not specify a version number of
this License, you may choose any version ever published by the Free Software
Foundation.

10. If you wish to incorporate parts of the Program into other free
programs whose distribution conditions are different, write to the author

to ask for permission. For software which is copyrighted by the Free
Software Foundation, write to the Free Software Foundation; we sometimes
make exceptions for this. Our decision will be guided by the two goals
of preserving the free status of all derivatives of our free software and
of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY
FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN

OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along

with this program; if not, write to the Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.
This
is free software, and you are welcome to redistribute it
under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than 'show w' and 'show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
'Gnomovision' (which makes passes at compilers) written by James Hacker.
<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License
does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this is what you want to do, use the GNU Lesser General
Public License instead of this License.

1.63 elfutils 0.166

1.63.1 Available under license :

GNU LESSER GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates

the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and the "GNU GPL" refers to version 3 of the GNU General Public License.

"The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An "Application" is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by
the Library is deemed a mode
of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the

function or data, the facility still operates, and performs
whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of
this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from
a header file that is part of the Library. You may convey such object
code under terms of your choice, provided that, if the incorporated
material is not limited to numerical parameters,
data structure
layouts and accessors, or small macros, inline functions and templates
(ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the
Library is used in it and that the Library and its use are
covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license
document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that,
taken together, effectively do not restrict modification of the
portions of the Library contained in the Combined Work and reverse
engineering for debugging such modifications, if you also do each of
the following:

a) Give prominent notice with each copy of the Combined Work that
the Library is used in it and that the Library and its use are
covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license
document.

c) For a Combined Work that
displays copyright notices during
execution, include the copyright notice for the Library among
these notices, as well as a reference directing the user to the
copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this
License, and the Corresponding Application Code in a form

suitable for, and under terms that permit, the user to
recombine or relink the Application with a modified version of
the Linked Version to produce a modified Combined Work, in the
manner specified by section 6 of the GNU GPL for conveying
Corresponding Source.

1) Use a suitable shared library mechanism for linking with the
Library. A suitable mechanism is one that (a) uses at run time
a copy of the Library already present on the user's computer
system, and (b) will operate properly with a modified version
of the Library that is interface-compatible
with the Linked
Version.

e) Provide Installation Information, but only if you would otherwise
be required to provide such information under section 6 of the
GNU GPL, and only to the extent that such information is
necessary to install and execute a modified version of the
Combined Work produced by recombining or relinking the
Application with a modified version of the Linked Version. (If
you use option 4d0, the Installation Information must accompany
the Minimal Corresponding Source and Corresponding Application
Code. If you use option 4d1, you must provide the Installation
Information in the manner specified by section 6 of the GNU GPL
for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the
Library side by side in a single library together with other library
facilities that are not Applications and are not covered by this
License, and convey such a combined
library under terms of your
choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based
on the Library, uncombined with any other library facilities,
conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it
is a work based on the Library, and explaining where to find the
accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions
of the GNU Lesser General Public License from time to time. Such new
versions will be similar in spirit to the present version, but may

differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price.
Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights.

These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program).

Whether that is true depends on what the
Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause
any work that you distribute or publish, that in
whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work
are not derived from the Program,
and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the

entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as

distribution of the source
code, even though third parties are not
compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing
or modifying
the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For
example, if a patent
license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE,
THERE IS NO WARRANTY
FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR
THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU
General Public License as published by
the Free Software Foundation; either version 2 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License along
with this program; if not, write to the Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute
it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this
is what you want to do, use the GNU Lesser General
Public License instead of this License.

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for
software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we

stand
ready to extend this provision to those domains in future versions
of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents.
States should not allow patents to restrict development and use of
software on general-purpose computers, but in those that do, we wish to
avoid the special danger that patents applied to a free program could
make it effectively proprietary. To prevent this, the GPL assures that
patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and
modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of
works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this
License. Each licensee is addressed as "you". "Licensees"
and
"recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work
in a fashion requiring copyright permission, other than the making of an
exact copy. The resulting work is called a "modified version" of the
earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based
on the Program.

To "propagate" a work means to do anything with it that, without
permission, would make you directly or secondarily liable for
infringement under applicable copyright law, except executing it on a
computer or modifying a private copy. Propagation includes copying,
distribution (with or without modification), making available to the
public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other
parties to make or receive copies. Mere interaction with a user through
a computer network, with no transfer of a copy, is
not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The
"System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally
available free
programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding

Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered
by this License only if the output, given its
content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed;
section 10
makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately
publish on each copy an appropriate copyright notice;
keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to
"keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution
medium, is called an
"aggregate" if the compilation and its resulting copyright are not

used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is

available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates

for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or

authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on

those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above
requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is

reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright
holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights
granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that

any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or

arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License,

section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE

USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17.
Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>
This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what you want to
do, use the GNU Lesser General
Public License instead of this License. But first, please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.

1.64 tcl 8.3.2

1.64.1 Available under license :

The author disclaims copyright to this source code. In place of
a legal notice, here is a blessing:

May you do good and not evil.
May you find forgiveness for yourself and forgive others.
May you share freely, never taking more than you give.
This is a mostly rewritten version of [incr Tcl], which is copyrighted
by Arnulf P. Wiedemann (c) Copyright 2008. It is derived from a version
written by Lucent Technologies, Inc., and other parties see that copyright
below.

The rewritten version is copyrighted with BSD license or Public Domain at
your choice.

The original version of this software is copyrighted by Lucent Technologies,
Inc., and other parties. The following terms apply to all files associated
with the software unless explicitly disclaimed in individual files.

The authors hereby grant permission to use, copy, modify, distribute,
and license this software and its documentation for any purpose, provided
that existing copyright notices are retained in all copies and that this
notice is included verbatim in any distributions. No written agreement,
license, or royalty fee is required for any of the authorized uses.
Modifications to this software may be copyrighted by their authors
and need not follow the licensing terms described
here, provided that
the new terms are clearly indicated on the first page of each file where
they apply.

IN NO EVENT SHALL THE AUTHORS OR DISTRIBUTORS BE LIABLE TO ANY PARTY
FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES
ARISING OUT OF THE USE OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY
DERIVATIVES THEREOF, EVEN IF THE AUTHORS HAVE BEEN ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

THE AUTHORS AND DISTRIBUTORS SPECIFICALLY DISCLAIM ANY WARRANTIES,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THIS SOFTWARE
IS PROVIDED ON AN "AS IS" BASIS, AND THE AUTHORS AND DISTRIBUTORS HAVE
NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR
MODIFICATIONS.

GOVERNMENT USE: If you are acquiring this software on behalf of the
U.S. government, the Government shall have only "Restricted Rights"
in the software and related documentation as defined in the Federal
Acquisition
Regulations (FARs) in Clause 52.227.19 (c) (2). If you
are acquiring the software on behalf of the Department of Defense, the
software shall be classified as "Commercial Computer Software" and the
Government shall have only "Restricted Rights" as defined in Clause
252.227-7013 (c) (1) of DFARs. Notwithstanding the foregoing, the
authors grant the U.S. Government and others acting in its behalf
permission to use and distribute the software in accordance with the
terms specified in this license.
This software is copyrighted by Kevin B. Kenny, and by other parties.
The following terms apply to all files associated with the software
unless explicitly disclaimed in individual files.

The authors hereby grant permission to use, copy, modify, distribute,
and license this software and its documentation for any purpose, provided
that existing copyright notices are retained in all copies and that this
notice is included verbatim in any distributions. No written agreement,
license, or royalty fee is required for any of the authorized uses.
Modifications to this software may be copyrighted by their authors
and need not follow the licensing terms described here, provided that
the new terms are clearly indicated on the first page of each file where

they apply.

IN NO EVENT SHALL THE AUTHORS OR DISTRIBUTORS BE LIABLE TO ANY PARTY
FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES
ARISING OUT OF THE USE OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY
DERIVATIVES THEREOF, EVEN IF
 THE AUTHORS HAVE BEEN ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

THE AUTHORS AND DISTRIBUTORS SPECIFICALLY DISCLAIM ANY WARRANTIES,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THIS SOFTWARE
IS PROVIDED ON AN "AS IS" BASIS, AND THE AUTHORS AND DISTRIBUTORS HAVE
NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR
MODIFICATIONS.

GOVERNMENT USE: If you are acquiring this software on behalf of the
U.S. government, the Government shall have only "Restricted Rights"
in the software and related documentation as defined in the Federal
Acquisition Regulations (FARs) in Clause 52.227.19 (c) (2). If you
are acquiring the software on behalf of the Department of Defense, the
software shall be classified as "Commercial Computer Software" and the
Government shall have only "Restricted Rights" as defined in Clause
252.227-7013 (c) (1) of DFARs. Notwithstanding the foregoing, the
authors grant
 the U.S. Government and others acting in its behalf
permission to use and distribute the software in accordance with the
terms specified in this license.

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>> [incr Tcl] <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

AUTHOR: Michael J. McLennan
       Bell Labs Innovations for Lucent Technologies
       mmclennan@lucent.com
       http://www.tcltk.com/itcl
==
         Copyright (c) 1993-1996 Lucent Technologies
==
Permission to use, copy, modify, and distribute this software and its
documentation for any purpose and without fee is hereby granted,
provided that the above copyright notice appear in all copies and that
both that the copyright notice and warranty disclaimer appear in
supporting documentation, and that the names of Lucent Technologies
any of their entities not be used in advertising or publicity
pertaining to distribution of the software without specific, written
prior permission.

Lucent Technologies

disclaims all warranties with regard to this
software, including all implied warranties of merchantability and
fitness. In no event shall Lucent be liable for any special, indirect
or consequential damages or any damages whatsoever resulting from loss
of use, data or profits, whether in an action of contract, negligence
or other tortuous action, arising out of or in connection with the use
or performance of this software.
==========

This software is copyrighted by Slawomir Cygan, and by other parties.
The following terms apply to all files associated with the software
unless explicitly disclaimed in individual files.

The authors hereby grant permission to use, copy, modify, distribute,
and license this software and its documentation for any purpose, provided
that existing copyright notices are retained in all copies and that this
notice is included verbatim in any distributions. No written agreement,
license, or royalty fee is required for any of the authorized uses.
Modifications to this software may be copyrighted by their authors
and need not follow the licensing terms described here, provided that
the new terms are clearly indicated on the first page of each file where
they apply.

IN NO EVENT SHALL THE AUTHORS OR DISTRIBUTORS BE LIABLE TO ANY PARTY
FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES
ARISING OUT OF THE USE OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY
DERIVATIVES THEREOF, EVEN IF
THE AUTHORS HAVE BEEN ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

THE AUTHORS AND DISTRIBUTORS SPECIFICALLY DISCLAIM ANY WARRANTIES,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THIS SOFTWARE
IS PROVIDED ON AN "AS IS" BASIS, AND THE AUTHORS AND DISTRIBUTORS HAVE
NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR
MODIFICATIONS.

GOVERNMENT USE: If you are acquiring this software on behalf of the
U.S. government, the Government shall have only "Restricted Rights"
in the software and related documentation as defined in the Federal
Acquisition Regulations (FARs) in Clause 52.227.19 (c) (2). If you
are acquiring the software on behalf of the Department of Defense, the
software shall be classified as "Commercial Computer Software" and the
Government shall have only "Restricted Rights" as defined in Clause
252.227-7013 (c) (1) of DFARs. Notwithstanding the foregoing, the
authors grant
the U.S. Government and others acting in its behalf
permission to use and distribute the software in accordance with the
terms specified in this license.

This software is copyrighted by Kevin B. Kenny, and by other parties.
The following terms apply to all files associated with the software
unless explicitly disclaimed in individual files.

The authors hereby grant permission to use, copy, modify, distribute,
and license this software and its documentation for any purpose, provided
that existing copyright notices are retained in all copies and that this
notice is included verbatim in any distributions. No written agreement,
license, or royalty fee is required for any of the authorized uses.
Modifications to this software may be copyrighted by their authors
and need not follow the licensing terms described here, provided that
the new terms are clearly indicated on the first page of each file where
they apply.

IN NO EVENT SHALL THE AUTHORS OR DISTRIBUTORS BE LIABLE TO ANY PARTY
FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES
ARISING OUT OF THE USE OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY
DERIVATIVES THEREOF, EVEN IF
THE AUTHORS HAVE BEEN ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

THE AUTHORS AND DISTRIBUTORS SPECIFICALLY DISCLAIM ANY WARRANTIES,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THIS SOFTWARE
IS PROVIDED ON AN "AS IS" BASIS, AND THE AUTHORS AND DISTRIBUTORS HAVE
NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR
MODIFICATIONS.

GOVERNMENT USE: If you are acquiring this software on behalf of the
U.S. government, the Government shall have only "Restricted Rights"
in the software and related documentation as defined in the Federal
Acquisition Regulations (FARs) in Clause 52.227.19 (c) (2). If you
are acquiring the software on behalf of the Department of Defense, the
software shall be classified as "Commercial Computer Software" and the
Government shall have only "Restricted Rights" as defined in Clause
252.227-7013 (c) (1) of DFARs. Notwithstanding the foregoing, the
authors grant
the U.S. Government and others acting in its behalf
permission to use and distribute the software in accordance with the
terms specified in this license.
This software is copyrighted by the Regents of the University of
California, Sun Microsystems, Inc., Scriptics Corporation,
and other parties. The following terms apply to all files associated
with the software unless explicitly disclaimed in individual files.

The authors hereby grant permission to use, copy, modify, distribute,
and license this software and its documentation for any purpose, provided
that existing copyright notices are retained in all copies and that this

notice is included verbatim in any distributions. No written agreement,
license, or royalty fee is required for any of the authorized uses.
Modifications to this software may be copyrighted by their authors
and need not follow the licensing terms described here, provided that
the new terms are clearly indicated on the first page of each file where
they apply.

IN NO EVENT SHALL THE AUTHORS OR DISTRIBUTORS BE LIABLE TO ANY PARTY
FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES
ARISING OUT OF THE USE
OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY
DERIVATIVES THEREOF, EVEN IF THE AUTHORS HAVE BEEN ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

THE AUTHORS AND DISTRIBUTORS SPECIFICALLY DISCLAIM ANY WARRANTIES,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THIS SOFTWARE
IS PROVIDED ON AN "AS IS" BASIS, AND THE AUTHORS AND DISTRIBUTORS HAVE
NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR
MODIFICATIONS.

GOVERNMENT USE: If you are acquiring this software on behalf of the
U.S. government, the Government shall have only "Restricted Rights"
in the software and related documentation as defined in the Federal
Acquisition Regulations (FARs) in Clause 52.227.19 (c) (2). If you
are acquiring the software on behalf of the Department of Defense, the
software shall be classified as "Commercial Computer Software" and the
Government shall have only "Restricted Rights" as defined in Clause
252.227-7013
(c) (1) of DFARs. Notwithstanding the foregoing, the
authors grant the U.S. Government and others acting in its behalf
permission to use and distribute the software in accordance with the
terms specified in this license.
Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization
obtaining a copy of the software and accompanying documentation covered by
this license (the "Software") to use, reproduce, display, distribute,
execute, and transmit the Software, and to prepare derivative works of the
Software, and to permit third-parties to whom the Software is furnished to
do so, all subject to the following:

The copyright notices in the Software and this entire statement, including
the above license grant, this restriction and the following disclaimer,
must be included in all copies of the Software, in whole or in part, and
all derivative works of the Software, unless such copies or derivative
works are solely in the form of machine-executable object code generated by
a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES
OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
This software is copyrighted by the Regents of the University of
California, Sun Microsystems, Inc., Scriptics Corporation, ActiveState
Corporation and other parties. The following terms apply to all files
associated with the software unless explicitly disclaimed in
individual files.

The authors hereby grant permission to use, copy, modify, distribute,
and license this software and its documentation for any purpose, provided
that existing copyright notices are retained in all copies and that this
notice is included verbatim in any distributions. No written agreement,
license, or royalty fee is required for any of the authorized uses.
Modifications to this software may be copyrighted by their authors
and need not follow the licensing terms described here, provided that
the new terms are clearly indicated on the first page of each file where
they apply.

IN NO EVENT SHALL THE AUTHORS OR DISTRIBUTORS BE LIABLE TO ANY PARTY
FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES
ARISING
OUT OF THE USE OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY
DERIVATIVES THEREOF, EVEN IF THE AUTHORS HAVE BEEN ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

THE AUTHORS AND DISTRIBUTORS SPECIFICALLY DISCLAIM ANY WARRANTIES,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THIS SOFTWARE
IS PROVIDED ON AN "AS IS" BASIS, AND THE AUTHORS AND DISTRIBUTORS HAVE
NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR
MODIFICATIONS.

GOVERNMENT USE: If you are acquiring this software on behalf of the
U.S. government, the Government shall have only "Restricted Rights"
in the software and related documentation as defined in the Federal
Acquisition Regulations (FARs) in Clause 52.227.19 (c) (2). If you
are acquiring the software on behalf of the Department of Defense, the
software shall be classified as "Commercial Computer Software" and the
Government shall have only "Restricted Rights" as
defined in Clause
252.227-7014 (b) (3) of DFARs. Notwithstanding the foregoing, the

authors grant the U.S. Government and others acting in its behalf
permission to use and distribute the software in accordance with the
terms specified in this license.
This software is copyrighted by the Scriptics Corporation, and other
parties. The following terms apply to all files associated with the
software unless explicitly disclaimed in individual files.

The authors hereby grant permission to use, copy, modify, distribute,
and license this software and its documentation for any purpose, provided
that existing copyright notices are retained in all copies and that this
notice is included verbatim in any distributions. No written agreement,
license, or royalty fee is required for any of the authorized uses.
Modifications to this software may be copyrighted by their authors
and need not follow the licensing terms described here, provided that
the new terms are clearly indicated on the first page of each file where
they apply.

IN NO EVENT SHALL THE AUTHORS OR DISTRIBUTORS BE LIABLE TO ANY PARTY
FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES
ARISING OUT OF THE USE OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY
DERIVATIVES THEREOF,
 EVEN IF THE AUTHORS HAVE BEEN ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

THE AUTHORS AND DISTRIBUTORS SPECIFICALLY DISCLAIM ANY WARRANTIES,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THIS SOFTWARE
IS PROVIDED ON AN "AS IS" BASIS, AND THE AUTHORS AND DISTRIBUTORS HAVE
NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR
MODIFICATIONS.

GOVERNMENT USE: If you are acquiring this software on behalf of the
U.S. government, the Government shall have only "Restricted Rights"
in the software and related documentation as defined in the Federal
Acquisition Regulations (FARs) in Clause 52.227.19 (c) (2). If you
are acquiring the software on behalf of the Department of Defense, the
software shall be classified as "Commercial Computer Software" and the
Government shall have only "Restricted Rights" as defined in Clause
252.227-7013 (c) (1) of DFARs. Notwithstanding the foregoing, the
authors
 grant the U.S. Government and others acting in its behalf
permission to use and distribute the software in accordance with the
terms specified in this license.

1.65 jansson 2.9

1.65.1 Available under license :

Copyright (c) 2009-2018 Petri Lehtinen <petri@digip.org>

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR
IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.

1.66 libdaemon 0.14

1.66.1 Available under license :

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts
as the successor of the GNU Library Public License, version 2, hence
the version number 2.1.]

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
Licenses are intended to guarantee your freedom to share and change
free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some
specially designated software packages--typically libraries--of the

Free Software Foundation and other authors who decide
to use it. You
can use it too, but we suggest you first think carefully about whether
this license or the ordinary General Public License is the better
strategy to use in any particular case, based on the explanations
below.

When we speak of free software, we are referring to freedom of use,
not price. Our General Public Licenses are designed to make sure that
you have the freedom to distribute copies of free software (and charge
for this service if you wish); that you receive source code or can get
it if you want it; that you can change the software and use pieces of
it in new free programs; and that you are informed that you can do
these things.

To protect your rights, we need to make restrictions that forbid
distributors to deny you these rights or to ask you to surrender these
rights. These restrictions translate to certain responsibilities for
you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether
gratis
or for a fee, you must give the recipients all the rights that we gave
you. You must make sure that they, too, receive or can get the source
code. If you link other code with the library, you must provide
complete object files to the recipients, so that they can relink them
with the library after making changes to the library and recompiling
it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the
library, and (2) we offer you this license, which gives you legal
permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that
there is no warranty for the free library. Also, if the library is
modified by someone else and passed on, the recipients should know
that what they have is not the original version, so that the original
author's reputation will not be affected by problems that might be
introduced by others.

Finally, software
patents pose a constant threat to the existence of
any free program. We wish to make sure that a company cannot
effectively restrict the users of a free program by obtaining a
restrictive license from a patent holder. Therefore, we insist that
any patent license obtained for a version of the library must be
consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits
such linking only if the
entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the
free library to free
software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The

former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to

exercise the right to control the distribution of derivative or
collective works based on the Library.

In addition, mere aggregation of another work not based on the Library
with the Library (or with a work based on the Library) on a volume of
a storage or distribution medium does not bring the other work under
the scope of this License.

3. You may opt to apply the terms of the ordinary
GNU General Public
License instead of this License to a given copy of the Library. To do
this, you must alter all the notices that refer to this License, so
that they refer to the ordinary GNU General Public License, version 2,
instead of to this License. (If a newer version than version 2 of the
ordinary GNU General Public License has appeared, then you can specify
that version instead if you wish.) Do not make any other change in
these notices.

Once this change is made in a given copy, it is irreversible for
that copy, so the ordinary GNU General Public License applies to all
subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of
the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or
derivative of it, under Section 2) in object code or executable form
under the terms of Sections 1 and 2 above provided that you accompany
it with the complete corresponding
machine-readable source code, which
must be distributed under the terms of Sections 1 and 2 above on a
medium customarily used for software interchange.

If distribution of object code is made by offering access to copy
from a designated place, then offering equivalent access to copy the
source code from the same place satisfies the requirement to
distribute the source code, even though third parties are not
compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the
Library, but is designed to work with the Library by being compiled or
linked with it, is called a "work that uses the Library". Such a
work, in isolation, is not a derivative work of the Library, and
therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library
creates an executable that is a derivative of the Library (because it
contains portions of the Library), rather than a "work that uses

the
library". The executable is therefore covered by this License.
Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object
code for the work under the terms of Section 6.
Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the
work with the complete corresponding
machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood

that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly
with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally
distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to

refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system
which is
implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish
revised and/or new
versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free

Software Foundation; we sometimes make exceptions for this. Our decision will
be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU
FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively
convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or
modify it under the terms of the GNU Lesser General Public
License as published by the Free Software Foundation; either
version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public
License along with this library; if not, write to the Free Software
Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301
USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or
your school, if any, to sign a "copyright disclaimer" for the library,
if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the
library `Frob' (a library for tweaking knobs) written by James
Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

1.67 busybox 1.24.1

1.67.1 Available under license :

GNU LESSER GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates
the terms and conditions of version 3 of the GNU General Public
License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and the "GNU GPL" refers to version 3 of the GNU General Public License.

"The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An "Application" is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by
the Library is deemed a mode
of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of
this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from
a header file that is part of the Library. You may convey such object
code under terms of your choice, provided that, if the incorporated
material is not limited to numerical parameters,
data structure
layouts and accessors, or small macros, inline functions and templates
(ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the
Library is used in it and that the Library and its use are
covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license
document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that,
taken together, effectively do not restrict modification of the
portions of the Library contained in the Combined Work and reverse
engineering for debugging such modifications, if you also do each of
the following:

a) Give prominent notice with each copy of the Combined Work that
the Library is used in it and that the Library and its use are
covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license
document.

c) For a Combined Work that
displays copyright notices during
execution, include the copyright notice for the Library among
these notices, as well as a reference directing the user to the
copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this
License, and the Corresponding Application Code in a form
suitable for, and under terms that permit, the user to
recombine or relink the Application with a modified version of

the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the
Library as you received it specifies that a certain numbered version
of the GNU Lesser General Public License "or any later version"
applies to it, you have the option
of following the terms and
conditions either of that published version or of any later version
published by the Free Software Foundation. If the Library as you
received it does not specify a version number of the GNU Lesser
General Public License, you may choose any version of the GNU Lesser
General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide
whether future versions of the GNU Lesser General Public License shall
apply, that proxy's public statement of acceptance of any version is
permanent authorization for you to choose that version for the
Library.
Copyright (c) 2015 Anton Skshidlevksy <meefik@gmail.com>

This program is free software: you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation, either version 3 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program. If not, see <http://www.gnu.org/licenses/>.

1.68 gdb 7.10.1

1.68.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free

software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed
to make sure that you
have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute
and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work
which contains
a notice placed by the copyright holder saying it may be distributed
under the terms of this General Public License. The "Program", below,
refers to any such program or work, and a "work based on the Program"
means either the Program or any derivative work under copyright law:
that is to say, a work containing the Program or a portion of it,
either verbatim or with modifications and/or translated into another
language. (Hereinafter, translation is included without limitation in
the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not
covered by this License; they are outside its scope. The act of
running the Program is not restricted, and the output from the Program
is covered only if its contents constitute a work based on the
Program (independent of having been made by running the Program).
Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim
copies of the Program's
source code as you receive it, in any medium, provided that you
conspicuously and appropriately publish on each copy an appropriate
copyright notice and disclaimer of warranty; keep intact all the
notices that refer to this License and to the absence of any warranty;
and give any other recipients of the Program a copy of this License
along with the Program.

You may charge a fee for the physical act of transferring a copy, and
you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion
of it, thus forming a work based on the Program, and copy and
distribute such modifications or work under the terms of Section 1
above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices
stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in

whole or in part contains or is derived from the Program or any
part thereof, to be licensed as a whole at no charge to all third
parties under the terms of this License.

c) If the modified program normally reads commands interactively
when run, you must cause it, when started running for such

interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably
considered independent and separate works in
themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work
based on it,
under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is

allowed only for noncommercial distribution and only if you
received the program in object code
or executable form with such
an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy
the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6.
Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version
number of this License which applies to it and "any
later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE
LAW. EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS),
EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest
to attach them to the start of each source file to most effectively
convey the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation; either version 2 of the
License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands
`show w' and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this is what you want to do, use the GNU Library General
Public License instead of this License.
@c The GNU Free Documentation License.
@center Version 1.3, 3 November 2008

@c This file is intended to be included within another document,
@c hence no sectioning command or @node.

@display
Copyright @copyright{} 2000, 2001, 2002, 2007, 2008 Free Software Foundation, Inc.
@uref{http://fsf.org/}

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.
@end display

@enumerate 0
@item
PREAMBLE

The purpose of this License is to make a manual, textbook, or other
functional and useful document @dfn{free} in the sense of freedom: to
assure everyone the effective freedom to copy and redistribute it,
with or without modifying it, either commercially or noncommercially.
Secondarily, this License preserves for the author and publisher a way
to get credit for their work, while not being considered responsible
for modifications made by others.

This License is a kind of ``copyleft'', which means that derivative
works of the document
 must themselves be free in the same sense. It
complements the GNU General Public License, which is a copyleft
license designed for free software.

We have designed this License in order to use it for manuals for free
software, because free software needs free documentation: a free
program should come with manuals providing the same freedoms that the
software does. But this License is not limited to software manuals;
it can be used for any textual work, regardless of subject matter or
whether it is published as a printed book. We recommend this License
principally for works whose purpose is instruction or reference.

@item
APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The ``Document'', below, refers
to any such manual or work. Any member of the public is a licensee, and is addressed as ``you''. You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A ``Modified Version'' of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A ``Secondary Section'' is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political
position regarding
them.

The ``Invariant Sections'' are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The ``Cover Texts'' are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A ``Transparent'' copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for

images composed of
pixels) generic paint programs or (for drawings) some widely available
drawing editor, and that is suitable for input to text formatters or
for automatic translation to a variety of formats suitable for input
to text formatters. A copy made in an otherwise Transparent file
format whose markup, or absence of markup, has been arranged to thwart
or discourage subsequent modification by readers is not Transparent.
An image format is not Transparent if used for any substantial amount
of text. A copy that is not ``Transparent'' is called ``Opaque''.

Examples of suitable formats for Transparent copies include plain
@sc{ascii} without markup, Texinfo input format, La@TeX{} input
format, @acronym{SGML} or @acronym{XML} using a publicly available
@acronym{DTD}, and standard-conforming simple @acronym{HTML},
PostScript or @acronym{PDF} designed for human modification. Examples
of transparent image formats include @acronym{PNG}, @acronym{XCF} and
@acronym{JPG}. Opaque formats
include proprietary formats that can be
read and edited only by proprietary word processors, @acronym{SGML} or
@acronym{XML} for which the @acronym{DTD} and/or processing tools are
not generally available, and the machine-generated @acronym{HTML},
PostScript or @acronym{PDF} produced by some word processors for
output purposes only.

The ``Title Page'' means, for a printed book, the title page itself,
plus such following pages as are needed to hold, legibly, the material
this License requires to appear in the title page. For works in
formats which do not have any title page as such, ``Title Page'' means
the text near the most prominent appearance of the work's title,
preceding the beginning of the body of the text.

The ``publisher'' means any person or entity that distributes copies
of the Document to the public.

A section ``Entitled XYZ'' means a named subunit of the Document whose
title either is precisely XYZ or contains XYZ in parentheses following
text that translates XYZ in
another language. (Here XYZ stands for a
specific section name mentioned below, such as ``Acknowledgements'',
``Dedications'', ``Endorsements'', or ``History''.) To ``Preserve the Title''
of such a section when you modify the Document means that it remains a
section ``Entitled XYZ'' according to this definition.

The Document may include Warranty Disclaimers next to the notice which
states that this License applies to the Document. These Warranty
Disclaimers are considered to be included by reference in this
License, but only as regards disclaiming warranties: any other
implication that these Warranty Disclaimers may have is void and has

no effect on the meaning of this License.

@item
VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever
to those of this License. You may not use
technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

@item
COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible.
You may add other material on the covers in addition.
Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps,

when you begin distribution of Opaque copies in quantity, to ensure
that
this Transparent copy will remain thus accessible at the stated
location until at least one year after the last time you distribute an
Opaque copy (directly or through your agents or retailers) of that
edition to the public.

It is requested, but not required, that you contact the authors of the
Document well before redistributing any large number of copies, to give
them a chance to provide you with an updated version of the Document.

@item
MODIFICATIONS

You may copy and distribute a Modified Version of the Document under
the conditions of sections 2 and 3 above, provided that you release
the Modified Version under precisely this License, with the Modified
Version filling the role of the Document, thus licensing distribution
and modification of the Modified Version to whoever possesses a copy
of it. In addition, you must do these things in the Modified Version:

@enumerate A
@item
Use in the Title Page (and on the covers, if any) a title distinct
from that of the Document, and from
those of previous versions
(which should, if there were any, be listed in the History section
of the Document). You may use the same title as a previous version
if the original publisher of that version gives permission.

@item
List on the Title Page, as authors, one or more persons or entities
responsible for authorship of the modifications in the Modified
Version, together with at least five of the principal authors of the
Document (all of its principal authors, if it has fewer than five),
unless they release you from this requirement.

@item
State on the Title page the name of the publisher of the
Modified Version, as the publisher.

@item
Preserve all the copyright notices of the Document.

@item
Add an appropriate copyright notice for your modifications
adjacent to the other copyright notices.

@item
Include, immediately after the copyright notices, a license notice
giving the public permission to use the Modified Version under the
terms of this License, in the form shown in
the Addendum below.

@item
Preserve in that license notice the full lists of Invariant Sections
and required Cover Texts given in the Document's license notice.

@item
Include an unaltered copy of this License.

@item
Preserve the section Entitled ``History'', Preserve its Title, and add
to it an item stating at least the title, year, new authors, and
publisher of the Modified Version as given on the Title Page. If
there is no section Entitled ``History'' in the Document, create one
stating the title, year, authors, and publisher of the Document as
given on its Title Page, then add an item describing the Modified
Version as stated in the previous sentence.

@item
Preserve the network location, if any, given in the Document for
public access to a Transparent copy of the Document, and likewise
the network locations given in the Document for previous versions
it was based on. These may be placed in the ``History'' section.
You may omit a network location for a work that was published at
least
four years before the Document itself, or if the original
publisher of the version it refers to gives permission.

@item
For any section Entitled ``Acknowledgements'' or ``Dedications'', Preserve
the Title of the section, and preserve in the section all the
substance and tone of each of the contributor acknowledgements and/or
dedications given therein.

@item
Preserve all the Invariant Sections of the Document,
unaltered in their text and in their titles. Section numbers
or the equivalent are not considered part of the section titles.

@item
Delete any section Entitled ``Endorsements''. Such a section
may not be included in the Modified Version.

@item

Do not retitle any existing section to be Entitled ``Endorsements'' or
to conflict in title with any Invariant Section.

@item
Preserve any Warranty Disclaimers.
@end enumerate

If the Modified Version includes new front-matter sections or
appendices that qualify as Secondary Sections and contain no material
copied from the Document,
you may at your option designate some or all
of these sections as invariant. To do this, add their titles to the
list of Invariant Sections in the Modified Version's license notice.
These titles must be distinct from any other section titles.

You may add a section Entitled ``Endorsements'', provided it contains
nothing but endorsements of your Modified Version by various
parties---for example, statements of peer review or that the text has
been approved by an organization as the authoritative definition of a
standard.

You may add a passage of up to five words as a Front-Cover Text, and a
passage of up to 25 words as a Back-Cover Text, to the end of the list
of Cover Texts in the Modified Version. Only one passage of
Front-Cover Text and one of Back-Cover Text may be added by (or
through arrangements made by) any one entity. If the Document already
includes a cover text for the same cover, previously added by you or
by arrangement made by the same entity you are acting on behalf
of,
you may not add another; but you may replace the old one, on explicit
permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License
give permission to use their names for publicity for or to assert or
imply endorsement of any Modified Version.

@item
COMBINING DOCUMENTS

You may combine the Document with other documents released under this
License, under the terms defined in section 4 above for modified
versions, provided that you include in the combination all of the
Invariant Sections of all of the original documents, unmodified, and
list them all as Invariant Sections of your combined work in its
license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and
multiple identical Invariant Sections may be replaced with a single

copy. If there are multiple Invariant Sections with the same name but
different contents, make the title of
 each such section unique by
adding at the end of it, in parentheses, the name of the original
author or publisher of that section if known, or else a unique number.
Make the same adjustment to the section titles in the list of
Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled ``History''
in the various original documents, forming one section Entitled
``History''; likewise combine any sections Entitled ``Acknowledgements'',
and any sections Entitled ``Dedications''. You must delete all
sections Entitled ``Endorsements.''

@item
COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents
released under this License, and replace the individual copies of this
License in the various documents with a single copy that is included in
the collection, provided that you follow the rules of this License for
verbatim copying of each of the documents in all other respects.

You may extract
 a single document from such a collection, and distribute
it individually under this License, provided you insert a copy of this
License into the extracted document, and follow this License in all
other respects regarding verbatim copying of that document.

@item
AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate
and independent documents or works, in or on a volume of a storage or
distribution medium, is called an ``aggregate'' if the copyright
resulting from the compilation is not used to limit the legal rights
of the compilation's users beyond what the individual works permit.
When the Document is included in an aggregate, this License does not
apply to the other works in the aggregate which are not themselves
derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these
copies of the Document, then if the Document is less than one half of
the entire aggregate, the Document's Cover Texts may
 be placed on
covers that bracket the Document within the aggregate, or the
electronic equivalent of covers if the Document is in electronic form.
Otherwise they must appear on printed covers that bracket the whole

aggregate.

@item
TRANSLATION

Translation is considered a kind of modification, so you may
distribute translations of the Document under the terms of section 4.
Replacing Invariant Sections with translations requires special
permission from their copyright holders, but you may include
translations of some or all Invariant Sections in addition to the
original versions of these Invariant Sections. You may include a
translation of this License, and all the license notices in the
Document, and any Warranty Disclaimers, provided that you also include
the original English version of this License and the original versions
of those notices and disclaimers. In case of a disagreement between
the translation and the original version of this License or a notice
or disclaimer, the original
 version will prevail.

If a section in the Document is Entitled ``Acknowledgements",
``Dedications", or ``History", the requirement (section 4) to Preserve
its Title (section 1) will typically require changing the actual
title.

@item
TERMINATION

You may not copy, modify, sublicense, or distribute the Document
except as expressly provided under this License. Any attempt
otherwise to copy, modify, sublicense, or distribute it is void, and
will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license
from a particular copyright holder is reinstated (a) provisionally,
unless and until the copyright holder explicitly and finally
terminates your license, and (b) permanently, if the copyright holder
fails to notify you of the violation by some reasonable means prior to
60 days after the cessation.

Moreover, your license from a particular copyright holder is
reinstated permanently if the copyright holder notifies
 you of the
violation by some reasonable means, this is the first time you have
received notice of violation of this License (for any work) from that
copyright holder, and you cure the violation prior to 30 days after
your receipt of the notice.

Termination of your rights under this section does not terminate the

licenses of parties who have received copies or rights from you under
this License. If your rights have been terminated and not permanently
reinstated, receipt of a copy of some or all of the same material does
not give you any rights to use it.

@item
FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions
of the GNU Free Documentation License from time to time. Such new
versions will be similar in spirit to the present version, but may
differ in detail to address new problems or concerns. See
@uref{http://www.gnu.org/copyleft/}.

Each version of the License is given a distinguishing version number.
If the Document specifies that
 a particular numbered version of this
License ``or any later version'' applies to it, you have the option of
following the terms and conditions either of that specified version or
of any later version that has been published (not as a draft) by the
Free Software Foundation. If the Document does not specify a version
number of this License, you may choose any version ever published (not
as a draft) by the Free Software Foundation. If the Document
specifies that a proxy can decide which future versions of this
License can be used, that proxy's public statement of acceptance of a
version permanently authorizes you to choose that version for the
Document.

@item
RELICENSING

``Massive Multiauthor Collaboration Site'' (or ``MMC Site'') means any
World Wide Web server that publishes copyrightable works and also
provides prominent facilities for anybody to edit those works. A
public wiki that anybody can edit is an example of such a server. A
``Massive Multiauthor Collaboration'' (or ``MMC'')
 contained in the
site means any set of copyrightable works thus published on the MMC
site.

``CC-BY-SA'' means the Creative Commons Attribution-Share Alike 3.0
license published by Creative Commons Corporation, a not-for-profit
corporation with a principal place of business in San Francisco,
California, as well as future copyleft versions of that license
published by that same organization.

``Incorporate'' means to publish or republish a Document, in whole or
in part, as part of another Document.

An MMC is ``eligible for relicensing'' if it is licensed under this
License, and if all works that were first published under this License
somewhere other than this MMC, and subsequently incorporated in whole
or in part into the MMC, (1) had no cover texts or invariant sections,
and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site
under CC-BY-SA on the same site at any time before August 1, 2009,
provided the
 MMC is eligible for relicensing.

@end enumerate

@page
@heading ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of
the License in the document and put the following copyright and
license notices just after the title page:

@smallexample
@group
 Copyright (C) @var{year} @var{your name}.
 Permission is granted to copy, distribute and/or modify this document
 under the terms of the GNU Free Documentation License, Version 1.3
 or any later version published by the Free Software Foundation;
 with no Invariant Sections, no Front-Cover Texts, and no Back-Cover
 Texts. A copy of the license is included in the section entitled ``GNU
 Free Documentation License''.
@end group
@end smallexample

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts,
replace the ``with@dots{}Texts.'' line with this:

@smallexample
@group
   with the Invariant Sections being @var{list their titles}, with
   the Front-Cover
 Texts being @var{list}, and with the Back-Cover Texts
   being @var{list}.
@end group
@end smallexample

If you have Invariant Sections without Cover Texts, or some other
combination of the three, merge those two alternatives to suit the
situation.

If your document contains nontrivial examples of program code, we
recommend releasing these examples in parallel under your choice of
free software license, such as the GNU General Public License,
to permit their use in free software.

@c Local Variables:
@c ispell-local-pdict: "ispell-dict"
@c End:

GNU LIBRARY GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the library GPL. It is
numbered 2 because it goes with version 2 of the ordinary GPL.]

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
Licenses are intended to guarantee your freedom to share and change
free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some
specially designated Free Software Foundation software, and to any
other libraries whose authors decide to use it. You can use it for
your libraries, too.

When we speak of free software, we are referring to freedom,
not
price. Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid
anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate to certain responsibilities for you if
you distribute copies of the library, or if you modify it.

For example, if you distribute copies of the library, whether gratis
or for a fee, you must give the recipients all the rights that we gave
you. You must make sure that they, too, receive or can get the source

code. If you link a program with the library, you must provide
complete object files to the recipients so that they can relink them
with the library, after making
 changes to the library and recompiling
it. And you must show them these terms so they know their rights.

 Our method of protecting your rights has two steps: (1) copyright
the library, and (2) offer you this license which gives you legal
permission to copy, distribute and/or modify the library.

 Also, for each distributor's protection, we want to make certain
that everyone understands that there is no warranty for this free
library. If the library is modified by someone else and passed on, we
want its recipients to know that what they have is not the original
version, so that any problems introduced by others will not reflect on
the original authors' reputations.

 Finally, any free program is threatened constantly by software
patents. We wish to avoid the danger that companies distributing free
software will individually obtain patent licenses, thus in effect
transforming the program into proprietary software. To prevent this,
we have made it clear that any patent must be licensed
 for everyone's
free use or not licensed at all.

 Most GNU software, including some libraries, is covered by the ordinary
GNU General Public License, which was designed for utility programs. This
license, the GNU Library General Public License, applies to certain
designated libraries. This license is quite different from the ordinary
one; be sure to read it in full, and don't assume that anything in it is
the same as in the ordinary license.

 The reason we have a separate public license for some libraries is that
they blur the distinction we usually make between modifying or adding to a
program and simply using it. Linking a program with a library, without
changing the library, is in some sense simply using the library, and is
analogous to running a utility program or application program. However, in
a textual and legal sense, the linked executable is a combined work, a
derivative of the original library, and the ordinary General Public License
treats it as such.

 Because
 of this blurred distinction, using the ordinary General
Public License for libraries did not effectively promote software
sharing, because most developers did not use the libraries. We
concluded that weaker conditions might promote sharing better.

 However, unrestricted linking of non-free programs would deprive the

users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

GNU LIBRARY GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not

covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent
of the use of the Library in a tool for
writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must
itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this
function must
be optional: if the application does not supply it, the square

root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition,
mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of
the
Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also compile or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by

this License. You must supply
a copy of this License. If the work
during execution displays copyright notices, you must include the
copyright notice for the Library among them, as well as a reference
directing the user to the copy of this License. Also, you must do one
of these things:

a) Accompany the work with the complete corresponding
machine-readable source code for the Library including whatever
changes were used in the work (which must be distributed under
Sections 1 and 2 above); and, if the work is an executable linked
with the Library, with the complete machine-readable "work that
uses the Library", as object code and/or source code, so that the
user can modify the Library and then relink to produce a modified
executable containing the modified Library. (It is understood
that the user who changes the contents of definitions files in the
Library will not necessarily be able to recompile the application
to use the modified definitions.)

b) Accompany the
work with a written offer, valid for at
least three years, to give the same user the materials
specified in Subsection 6a, above, for a charge no more
than the cost of performing this distribution.

c) If distribution of the work is made by offering access to copy
from a designated place, offer equivalent access to copy the above
specified materials from the same place.

d) Verify that the user has already received a copy of these
materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the
Library" must include any data and utility programs needed for
reproducing the executable from it. However, as a special exception,
the source code distributed need not include anything that is normally
distributed (in either source or binary form) with the major
components (compiler, kernel, and so on) of the operating system on
which the executable runs, unless that component itself accompanies
the executable.

It may happen that this requirement contradicts the license
restrictions of other proprietary libraries that do not normally
accompany the operating system. Such a contradiction means you cannot
use both them and the Library together in an executable that you
distribute.

7. You may place library facilities that are a work based on the

Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this

License and any other pertinent obligations, then as a consequence you may not distribute
the Library at all. For example, if a patent
license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system;
it is up to the author/donor to decide if he or she is willing
to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Library General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each
version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY
IS LICENSED FREE OF CHARGE, THERE IS NO
WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR
LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A
FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Appendix: How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the

"copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year>
<name of author>

This library is free software; you can redistribute it and/or
modify it under the terms of the GNU Library General Public
License as published by the Free Software Foundation; either
version 2 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
Library General Public License for more details.

You should have received a copy of the GNU Library General Public
License along with this library; if not, write to the Free
Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston,
MA 02110-1301, USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the library, if
necessary.
Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the
library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!
GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts
as the successor of the GNU Library Public License, version 2, hence
the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we
suggest you first think carefully about whether
this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the
recipients all the rights that we gave
you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence

of
any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination
fits its criteria of freedom. The Lesser General
Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we
use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the

users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without
limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that

you conspicuously and appropriately publish
on each copy an
appropriate copyright notice and disclaimer of warranty; keep intact
all the notices that refer to this License and to the absence of any
warranty; and distribute a copy of this License along with the
Library.

You may charge a fee for the physical act of transferring a copy,
and you may at your option offer warranty protection in exchange for a
fee.

2. You may modify your copy or copies of the Library or any portion
of it, thus forming a work based on the Library, and copy and
distribute such modifications or work under the terms of Section 1
above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices
stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no
charge to all third parties under the terms of this License.

d) If a facility in the modified
Library refers to a function or a
table of data to be supplied by an application program that uses
the facility, other than as an argument passed when the facility
is invoked, then you must make a good faith effort to ensure that,
in the event an application does not supply such function or
table, the facility still operates, and performs whatever part of
its purpose remains meaningful.

(For example, a function in a library to compute square roots has
a purpose that is entirely well-defined independent of the
application. Therefore, Subsection 2d requires that any
application-supplied function or table used by this function must
be optional: if the application does not supply it, the square
root function must still compute square roots.)

These requirements apply to the modified work as a whole. If
identifiable sections of that work are not derived from the Library,
and can be reasonably considered independent and separate works in
themselves,
then this License, and its terms, do not apply to those
sections when you distribute them as separate works. But when you
distribute the same sections as part of a whole which is a work based
on the Library, the distribution of the whole must be on the terms of

this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a

work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License.
Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable

source code for the Library including whatever
changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the
user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major
components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot

distribute
so as to satisfy simultaneously your obligations under this
License and any other pertinent obligations, then as a consequence you
may not distribute the Library at all. For example, if a patent
license would not permit royalty-free redistribution of the Library by
all those who receive copies directly or indirectly through you, then
the only way you could satisfy both it and this License would be to
refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any
particular circumstance, the balance of the section is intended to apply,
and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any
patents or other property right claims or to contest validity of any
such claims; this section has the sole purpose of protecting the
integrity of the free software distribution system which is
implemented by public license practices. Many
people have made
generous contributions to the wide range of software distributed
through that system in reliance on consistent application of that
system; it is up to the author/donor to decide if he or she is willing
to distribute software through any other system and a licensee cannot
impose that choice.

This section is intended to make thoroughly clear what is believed to
be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in
certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Library under this License may add
an explicit geographical distribution limitation excluding those countries,
so that distribution is permitted only in or among countries not thus
excluded. In such case, this License incorporates the limitation as if
written in the body of this License.

13. The Free Software Foundation may publish revised and/or new
versions of the Lesser General Public
License from time to time.
Such new versions will be similar in spirit to the present version,
but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library
specifies a version number of this License which applies to it and
"any later version", you have the option of following the terms and
conditions either of that version or of any later version published by
the Free Software Foundation. If the Library does not specify a
license version number, you may choose any version ever published by

the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status
of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL
DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively

convey the exclusion of warranty; and each file should have at least the
"copyright" line
and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or
modify it under the terms of the GNU Lesser General Public
License as published by the Free Software Foundation; either
version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public
License along with this library; if not, write to the Free Software
Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You
should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the library, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the
library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!
GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for
software and other kinds of works.

The licenses for most software and other practical works are designed

to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand

ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices"

to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately
publish on each copy an appropriate copyright notice;
keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to
"keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution
medium, is called an
"aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users

beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for

the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on

those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above
requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the

violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright
holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights
granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for

sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a

covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the

combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF

DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17.
Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short

notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>
This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what you want to
do, use the GNU Lesser General
Public License instead of this License. But first, please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.
GNU LESSER GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates
the terms and conditions of version 3 of the GNU General Public
License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, "this License" refers to version 3 of the GNU Lesser
General Public License, and the "GNU GPL" refers to version 3 of the GNU
General Public License.

"The Library" refers to a covered work governed by this License,
other than an Application or a Combined Work as defined below.

An "Application" is any work that makes use of an interface provided
by the Library, but which is not otherwise based on the Library.
Defining a subclass of a class defined by the Library is

deemed a mode
of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying
Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data
structure
layouts and accessors, or small macros, inline functions and templates

(ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide

```
whether future versions of the GNU Lesser General Public License shall
apply, that proxy's public statement of acceptance of any version is
permanent authorization for you to choose that version for the
Library.
BEGIN {
  FS="\"";
  print "/* ==> Do not modify this file!!  " \
  "-*- buffer-read-only: t -*- vi" \
  ":set ro:";
  print "   It is created automatically by copying.awk.";
  print "   Modify copying.awk instead.  <== */";
  print ""
  print "#include \"defs.h\""
  print "#include \"command.h\""
  print "#include \"gdbcmd.h\""
  print ""
  print "static void show_copying_command (char *, int);"
  print ""
  print "static void show_warranty_command (char *, int);"
  print ""
  print "void _initialize_copying (void);"
  print ""
  print "static void";
  print "show_copying_command (char *ignore, int from_tty)";
  print "{";
 }
NR == 1,/^[  ]*15\. Disclaimer of Warranty\.[  ]*$/ {
  if ($0 ~ //)
    {
      printf "  printf_filtered (\"\\n\");\n";
    }
  else if ($0 !~ /^[  ]*15\. Disclaimer of Warranty\.[  ]*$/)
    {
      printf "  printf_filtered (\"";
      for (i = 1; i < NF; i++)
  printf "%s\\\"", $i;
      printf "%s\\n\");\n", $NF;
    }
 }
/^[  ]*15\.
 Disclaimer of Warranty\.[  ]*$/ {
  print "}";
  print "";
  print "static void";
  print "show_warranty_command (char *ignore, int from_tty)";
  print "{";
 }
/^[  ]*15\. Disclaimer of Warranty\.[  ]*$/, /^[  ]*END OF TERMS AND CONDITIONS[  ]*$/{
```

```
  if (! ($0 ~ /^[  ]*END OF TERMS AND CONDITIONS[  ]*$/))
    {
      printf "  printf_filtered (\"";
      for (i = 1; i < NF; i++)
  printf "%s\\\"", $i;
      printf "%s\\n\");\n", $NF;
    }
 }
END {
  print "}";
  print "";
  print "void"
  print "_initialize_copying (void)";
  print "{";
  print "  add_cmd (\"copying\", no_set_class, show_copying_command,";
  print "    _(\"Conditions for redistributing copies of GDB.\"),";
  print "    &showlist);";
  print "  add_cmd (\"warranty\", no_set_class, show_warranty_command,";
  print "    _(\"Various kinds of warranty you do not have.\"),";
  print "    &showlist);";
  print "";
  print "  /* For old-timers, allow \"info copying\", etc.  */";
  print "  add_info
 (\"copying\", show_copying_command,";
  print "     _(\"Conditions for redistributing copies of GDB.\"));";
  print "  add_info (\"warranty\", show_warranty_command,";
  print "     _(\"Various kinds of warranty you do not have.\"));";
  print "}";
 }
```

Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization
obtaining a copy of the software and accompanying documentation covered by
this license (the "Software") to use, reproduce, display, distribute,
execute, and transmit the Software, and to prepare derivative works of the
Software, and to permit third-parties to whom the Software is furnished to
do so, all subject to the following:

The copyright notices in the Software and this entire statement, including
the above license grant, this restriction and the following disclaimer,
must be included in all copies of the Software, in whole or in part, and
all derivative works of the Software, unless such copies or derivative
works are solely in the form of machine-executable object code generated by
a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES

OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
@node Library Copying
@appendixsec GNU LESSER GENERAL PUBLIC LICENSE

@cindex LGPL, Lesser General Public License
@center Version 2.1, February 1999

@display
Copyright @copyright{} 1991, 1999 Free Software Foundation, Inc.
51 Franklin Street - Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts
as the successor of the GNU Library Public License, version 2, hence the
version number 2.1.]
@end display

@appendixsubsec Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
Licenses are intended to guarantee your freedom to share and change
free software---to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some
specially designated software---typically libraries---of
the Free
Software Foundation and other authors who decide to use it. You can use
it too, but we suggest you first think carefully about whether this
license or the ordinary General Public License is the better strategy to
use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use,
not price. Our General Public Licenses are designed to make sure that
you have the freedom to distribute copies of free software (and charge
for this service if you wish); that you receive source code or can get
it if you want it; that you can change the software and use pieces of it
in new free programs; and that you are informed that you can do these
things.

To protect your rights, we need to make restrictions that forbid

distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems
that might be
introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library.
The ordinary
General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the @dfn{Lesser} General Public License because it

does @emph{Less} to protect the user's freedom than the ordinary General
Public License. It also provides other free software developers Less
of an advantage over competing non-free programs. These disadvantages
are the reason we use the ordinary General Public License for many
libraries. However, the Lesser license provides advantages in certain
special circumstances.

For example, on rare occasions, there may be a special need to
encourage the widest possible use of a certain library, so that it becomes
a de-facto standard. To achieve this, non-free programs must be
allowed to use the library. A more frequent case is that a free
library does the same job as widely used non-free
libraries. In this
case, there is little to gain by limiting the free library to free
software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free
programs enables a greater number of people to use a large body of
free software. For example, permission to use the GNU C Library in
non-free programs enables many more people to use the whole GNU
operating system, as well as its variant, the GNU/Linux operating
system.

Although the Lesser General Public License is Less protective of the
users' freedom, it does ensure that the user of a program that is
linked with the Library has the freedom and the wherewithal to run
that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and
modification follow. Pay close attention to the difference between a
``work based on the library'' and a ``work that uses the library''. The
former contains code derived from the
library, whereas the latter must
be combined with the library in order to run.

@iftex
@appendixsubsec TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION
@end iftex
@ifinfo
@center GNU LESSER GENERAL PUBLIC LICENSE
@center TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION
@end ifinfo

@enumerate 0
@item
This License Agreement applies to any software library or other program
which contains a notice placed by the copyright holder or other
authorized party saying it may be distributed under the terms of this

Lesser General Public License (also called ``this License''). Each licensee is addressed as ``you''.

A ``library'' means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The ``Library'', below, refers to any such software library or work which has been distributed under these terms. A ``work based on the Library'' means
either the Library or any derivative work under
copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term ``modification''.)

``Source code'' for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether
that is true depends on what the Library does
and what the program that uses the Library does.

@item
You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

@item
You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1

above, provided that you also meet all of these conditions:

@enumerate a
@item
The modified work must itself be a software library.

@item
You must cause
the files modified to carry prominent notices
stating that you changed the files and the date of any change.

@item
You must cause the whole of the work to be licensed at no
charge to all third parties under the terms of this License.

@item
If a facility in the modified Library refers to a function or a
table of data to be supplied by an application program that uses
the facility, other than as an argument passed when the facility
is invoked, then you must make a good faith effort to ensure that,
in the event an application does not supply such function or
table, the facility still operates, and performs whatever part of
its purpose remains meaningful.

(For example, a function in a library to compute square roots has
a purpose that is entirely well-defined independent of the
application. Therefore, Subsection 2d requires that any
application-supplied function or table used by this function must
be optional: if the application does not supply it, the square
root function must still
compute square roots.)
@end enumerate

These requirements apply to the modified work as a whole. If
identifiable sections of that work are not derived from the Library,
and can be reasonably considered independent and separate works in
themselves, then this License, and its terms, do not apply to those
sections when you distribute them as separate works. But when you
distribute the same sections as part of a whole which is a work based
on the Library, the distribution of the whole must be on the terms of
this License, whose permissions for other licensees extend to the
entire whole, and thus to each and every part regardless of who wrote
it.

Thus, it is not the intent of this section to claim rights or contest
your rights to work written entirely by you; rather, the intent is to
exercise the right to control the distribution of derivative or
collective works based on the Library.

In addition, mere aggregation of another work not based on the Library
with the Library (or with a work
 based on the Library) on a volume of
a storage or distribution medium does not bring the other work under
the scope of this License.

@item
You may opt to apply the terms of the ordinary GNU General Public
License instead of this License to a given copy of the Library. To do
this, you must alter all the notices that refer to this License, so
that they refer to the ordinary GNU General Public License, version 2,
instead of to this License. (If a newer version than version 2 of the
ordinary GNU General Public License has appeared, then you can specify
that version instead if you wish.) Do not make any other change in
these notices.

 Once this change is made in a given copy, it is irreversible for
that copy, so the ordinary GNU General Public License applies to all
subsequent copies and derivative works made from that copy.

 This option is useful when you wish to copy part of the code of
the Library into a program that is not a library.

@item
You may copy and distribute the Library
 (or a portion or
derivative of it, under Section 2) in object code or executable form
under the terms of Sections 1 and 2 above provided that you accompany
it with the complete corresponding machine-readable source code, which
must be distributed under the terms of Sections 1 and 2 above on a
medium customarily used for software interchange.

 If distribution of object code is made by offering access to copy
from a designated place, then offering equivalent access to copy the
source code from the same place satisfies the requirement to
distribute the source code, even though third parties are not
compelled to copy the source along with the object code.

@item
A program that contains no derivative of any portion of the
Library, but is designed to work with the Library by being compiled or
linked with it, is called a ``work that uses the Library". Such a
work, in isolation, is not a derivative work of the Library, and
therefore falls outside the scope of this License.

 However,

linking a ``work that uses the Library'' with the Library
creates an executable that is a derivative of the Library (because it
contains portions of the Library), rather than a ``work that uses the
library''. The executable is therefore covered by this License.
Section 6 states terms for distribution of such executables.

When a ``work that uses the Library'' uses material from a header file
that is part of the Library, the object code for the work may be a
derivative work of the Library even though the source code is not.
Whether this is true is especially significant if the work can be
linked without the Library, or if the work is itself a library. The
threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data
structure layouts and accessors, and small macros and small inline
functions (ten lines or less in length), then the use of the object
file is unrestricted, regardless of whether it is legally a derivative
work.
(Executables containing this object code plus portions of the
Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may
distribute the object code for the work under the terms of Section 6.
Any executables containing that work also fall under Section 6,
whether or not they are linked directly with the Library itself.

@item
As an exception to the Sections above, you may also combine or
link a ``work that uses the Library'' with the Library to produce a
work containing portions of the Library, and distribute that work
under terms of your choice, provided that the terms permit
modification of the work for the customer's own use and reverse
engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the
Library is used in it and that the Library and its use are covered by
this License. You must supply a copy of this License. If the work
during execution displays copyright notices,
you must include the
copyright notice for the Library among them, as well as a reference
directing the user to the copy of this License. Also, you must do one
of these things:

@enumerate a
@item
Accompany the work with the complete corresponding
machine-readable source code for the Library including whatever
changes were used in the work (which must be distributed under

Sections 1 and 2 above); and, if the work is an executable linked
with the Library, with the complete machine-readable ``work that
uses the Library'', as object code and/or source code, so that the
user can modify the Library and then relink to produce a modified
executable containing the modified Library. (It is understood
that the user who changes the contents of definitions files in the
Library will not necessarily be able to recompile the application
to use the modified definitions.)

@item
Use a suitable shared library mechanism for linking with the Library. A
suitable mechanism is one that (1) uses at run time
 a copy of the
library already present on the user's computer system, rather than
copying library functions into the executable, and (2) will operate
properly with a modified version of the library, if the user installs
one, as long as the modified version is interface-compatible with the
version that the work was made with.

@item
Accompany the work with a written offer, valid for at
least three years, to give the same user the materials
specified in Subsection 6a, above, for a charge no more
than the cost of performing this distribution.

@item
If distribution of the work is made by offering access to copy
from a designated place, offer equivalent access to copy the above
specified materials from the same place.

@item
Verify that the user has already received a copy of these
materials or that you have already sent this user a copy.
@end enumerate

 For an executable, the required form of the ``work that uses the
Library'' must include any data and utility programs needed for
reproducing
 the executable from it. However, as a special exception,
the materials to be distributed need not include anything that is
normally distributed (in either source or binary form) with the major
components (compiler, kernel, and so on) of the operating system on
which the executable runs, unless that component itself accompanies the
executable.

 It may happen that this requirement contradicts the license
restrictions of other proprietary libraries that do not normally
accompany the operating system. Such a contradiction means you cannot

use both them and the Library together in an executable that you
distribute.

@item
You may place library facilities that are a work based on the
Library side-by-side in a single library together with other library
facilities not covered by this License, and distribute such a combined
library, provided that the separate distribution of the work based on
the Library and of the other library facilities is otherwise
permitted, and provided that
 you do these two things:

@enumerate a
@item
Accompany the combined library with a copy of the same work
based on the Library, uncombined with any other library
facilities. This must be distributed under the terms of the
Sections above.

@item
Give prominent notice with the combined library of the fact
that part of it is a work based on the Library, and explaining
where to find the accompanying uncombined form of the same work.
@end enumerate

@item
You may not copy, modify, sublicense, link with, or distribute
the Library except as expressly provided under this License. Any
attempt otherwise to copy, modify, sublicense, link with, or
distribute the Library is void, and will automatically terminate your
rights under this License. However, parties who have received copies,
or rights, from you under this License will not have their licenses
terminated so long as such parties remain in full compliance.

@item
You are not required to accept this License, since you have not
signed it. However,
 nothing else grants you permission to modify or
distribute the Library or its derivative works. These actions are
prohibited by law if you do not accept this License. Therefore, by
modifying or distributing the Library (or any work based on the
Library), you indicate your acceptance of this License to do so, and
all its terms and conditions for copying, distributing or modifying
the Library or works based on it.

@item
Each time you redistribute the Library (or any work based on the
Library), the recipient automatically receives a license from the

original licensor to copy, distribute, link with or modify the Library
subject to these terms and conditions. You may not impose any further
restrictions on the recipients' exercise of the rights granted herein.
You are not responsible for enforcing compliance by third parties with
this License.

@item
If, as a consequence of a court judgment or allegation of patent
infringement or for any other reason (not limited to patent issues),
conditions
 are imposed on you (whether by court order, agreement or
otherwise) that contradict the conditions of this License, they do not
excuse you from the conditions of this License. If you cannot
distribute so as to satisfy simultaneously your obligations under this
License and any other pertinent obligations, then as a consequence you
may not distribute the Library at all. For example, if a patent
license would not permit royalty-free redistribution of the Library by
all those who receive copies directly or indirectly through you, then
the only way you could satisfy both it and this License would be to
refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any
particular circumstance, the balance of the section is intended to apply,
and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any
patents or other property right claims
 or to contest validity of any
such claims; this section has the sole purpose of protecting the
integrity of the free software distribution system which is
implemented by public license practices. Many people have made
generous contributions to the wide range of software distributed
through that system in reliance on consistent application of that
system; it is up to the author/donor to decide if he or she is willing
to distribute software through any other system and a licensee cannot
impose that choice.

This section is intended to make thoroughly clear what is believed to
be a consequence of the rest of this License.

@item
If the distribution and/or use of the Library is restricted in
certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Library under this License may add
an explicit geographical distribution limitation excluding those countries,
so that distribution is permitted only in or among countries not thus
excluded.

In such case, this License incorporates the limitation as if
written in the body of this License.

@item
The Free Software Foundation may publish revised and/or new
versions of the Lesser General Public License from time to time.
Such new versions will be similar in spirit to the present version,
but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library
specifies a version number of this License which applies to it and
``any later version'', you have the option of following the terms and
conditions either of that version or of any later version published by
the Free Software Foundation. If the Library does not specify a
license version number, you may choose any version ever published by
the Free Software Foundation.

@item
If you wish to incorporate parts of the Library into other free
programs whose distribution conditions are incompatible with these,
write to the author to ask for permission. For software
which is
copyrighted by the Free Software Foundation, write to the Free
Software Foundation; we sometimes make exceptions for this. Our
decision will be guided by the two goals of preserving the free status
of all derivatives of our free software and of promoting the sharing
and reuse of software generally.

@center NO WARRANTY

@item
BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO
WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW.
EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR
OTHER PARTIES PROVIDE THE LIBRARY ``AS IS'' WITHOUT WARRANTY OF ANY
KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE
LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME
THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

@item
IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED
TO IN
WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY
AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU
FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR
CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE

LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
@end enumerate

@iftex
@heading END OF TERMS AND CONDITIONS
@end iftex
@ifinfo
@center END OF TERMS AND CONDITIONS
@end ifinfo

@page
@appendixsubsec How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the ``copyright'' line and a pointer to where the full notice is found.

@smallexample
@var{one line to give the library's name and an idea of what it does.}
Copyright (C) @var{year} @var{name of author}

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.

@end smallexample

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a ``copyright disclaimer'' for the library, if
necessary. Here is a sample; alter the names:

@smallexample
Yoyodyne, Inc., hereby disclaims all copyright interest in the library
`Frob' (a library for tweaking knobs) written by James Random Hacker.

@var{signature of Ty Coon}, 1 April 1990
Ty Coon, President of Vice
@end smallexample

That's all there is to it!
#! /usr/bin/env python

Copyright (C) 2011-2015 Free Software Foundation, Inc.
#
This file is part of GDB.
#
This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation; either version 3 of the License, or
(at your option) any later version.
#
This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.
#
You should have received a copy of the GNU General Public License
along with this program. If not, see <http://www.gnu.org/licenses/>.

"""copyright.py

This script updates the list of years in the copyright notices in
most files maintained by the GDB project.

Usage: cd src/gdb && python copyright.py

Always review the output of this script before committing it!
A useful command to review
 the output is:
   % filterdiff -x *.c -x *.cc -x *.h -x *.exp updates.diff
This removes the bulk of the changes which are most likely to be correct.

```
"""

import datetime
import os
import os.path
import subprocess


def get_update_list():
  """Return the list of files to update.

  Assumes that the current working directory when called is the root
  of the GDB source tree (NOT the gdb/ subdirectory!).  The names of
  the files are relative to that root directory.
  """
  result = []
  for gdb_dir in ('gdb', 'sim', 'include/gdb'):
     for root, dirs, files in os.walk(gdb_dir, topdown=True):
        for dirname in dirs:
           reldirname = "%s/%s" % (root, dirname)
           if (dirname in EXCLUDE_ALL_LIST
              or reldirname in EXCLUDE_LIST
              or reldirname in NOT_FSF_LIST
              or reldirname in BY_HAND):
              # Prune this directory from our search list.
              dirs.remove(dirname)
         for filename in files:
           relpath = "%s/%s" % (root, filename)
           if (filename in EXCLUDE_ALL_LIST
              or relpath in EXCLUDE_LIST
              or relpath in NOT_FSF_LIST
              or relpath in BY_HAND):
              # Ignore this file.
              pass
           else:
              result.append(relpath)
  return result


def update_files(update_list):
  """Update the copyright header of the files in the given list.

  We use gnulib's update-copyright script for that.
  """
  # We want to use year intervals in the copyright notices, and
  # all years should be collapsed to one single year interval,
  # even if there are "holes" in the list of years found in the
  # original copyright notice (OK'ed by the FSF, case [gnu.org #719834]).
```

```
  os.environ['UPDATE_COPYRIGHT_USE_INTERVALS'] = '2'

  # Perform the update, and save the output in a string.
  update_cmd
= ['bash', 'gdb/gnulib/import/extra/update-copyright']
  update_cmd += update_list

  p = subprocess.Popen(update_cmd, stdout=subprocess.PIPE,
                       stderr=subprocess.STDOUT)
  update_out = p.communicate()[0]

  # Process the output.  Typically, a lot of files do not have
  # a copyright notice :-(.  The update-copyright script prints
  # a well defined warning when it did not find the copyright notice.
  # For each of those, do a sanity check and see if they may in fact
  # have one.  For the files that are found not to have one, we filter
  # the line out from the output, since there is nothing more to do,
  # short of looking at each file and seeing which notice is appropriate.
  # Too much work! (~4,000 files listed as of 2012-01-03).
  update_out = update_out.splitlines()
  warning_string = ': warning: copyright statement not found'
  warning_len = len(warning_string)

  for line in update_out:
     if line.endswith('\n'):

      line = line[:-1]
     if line.endswith(warning_string):
        filename = line[:-warning_len]
        if may_have_copyright_notice(filename):
           print line
     else:
        # Unrecognized file format. !?!
        print "*** " + line


def may_have_copyright_notice(filename):
  """Check that the given file does not seem to have a copyright notice.

  The filename is relative to the root directory.
  This function assumes that the current working directory is that root
  directory.

  The algorigthm is fairly crude, meaning that it might return
  some false positives.  I do not think it will return any false
  negatives...  We might improve this function to handle more
  complex cases later...
  """
```

```
  # For now, it may have a copyright notice if we find the word
  # "Copyright" at the (reasonable) start of the given file, say
  # 50 lines...
  MAX_LINES = 50

  fd = open(filename)

  lineno = 1
  for line in fd:
      if 'Copyright' in line:
         return True
      lineno += 1
      if lineno > 50:
         return False
  return False


def main ():
  """The main subprogram."""
  if not os.path.isfile("gnulib/import/extra/update-copyright"):
      print "Error: This script must be called from the gdb directory."
  root_dir = os.path.dirname(os.getcwd())
  os.chdir(root_dir)

  update_list = get_update_list()
  update_files (update_list)

  # Remind the user that some files need to be updated by HAND...
  if BY_HAND:
      print
      print "\033[31mREMINDER: The following files must be updated by hand." \
          "\033[0m"
      for filename in BY_HAND + MULTIPLE_COPYRIGHT_HEADERS:
         print "  ", filename

################################################################################
#
# Some constants, placed at the end because they take up a lot of room.
# The actual value of these constants is not significant to the understanding
# of the
 script.
#
################################################################################

# Files which should not be modified, either because they are
# generated, non-FSF, or otherwise special (e.g. license text,
# or test cases which must be sensitive to line numbering).
#
```

```
# Filenames are relative to the root directory.
EXCLUDE_LIST = (
  'gdb/nat/glibc_thread_db.h',
  'gdb/CONTRIBUTE',
  'gdb/gnulib/import'
)

# Files which should not be modified, either because they are
# generated, non-FSF, or otherwise special (e.g. license text,
# or test cases which must be sensitive to line numbering).
#
# Matches any file or directory name anywhere.  Use with caution.
# This is mostly for files that can be found in multiple directories.
# Eg: We want all files named COPYING to be left untouched.

EXCLUDE_ALL_LIST = (
  "COPYING", "COPYING.LIB", "CVS", "configure", "copying.c",
  "fdl.texi", "gpl.texi", "aclocal.m4",
)

# The list of files to update by hand.
BY_HAND = (
  # These
 files are sensitive to line numbering.
  "gdb/testsuite/gdb.base/step-line.inp",
  "gdb/testsuite/gdb.base/step-line.c",
)

# Files containing multiple copyright headers.  This script is only
# fixing the first one it finds, so we need to finish the update
# by hand.
MULTIPLE_COPYRIGHT_HEADERS = (
  "gdb/doc/gdb.texinfo",
  "gdb/doc/refcard.tex",
  "gdb/gdbarch.sh",
)

# The list of file which have a copyright, but not head by the FSF.
# Filenames are relative to the root directory.
NOT_FSF_LIST = (
  "gdb/exc_request.defs",
  "gdb/gdbtk",
  "gdb/testsuite/gdb.gdbtk/",
  "sim/arm/armemu.h", "sim/arm/armos.c", "sim/arm/gdbhost.c",
  "sim/arm/dbg_hif.h", "sim/arm/dbg_conf.h", "sim/arm/communicate.h",
  "sim/arm/armos.h", "sim/arm/armcopro.c", "sim/arm/armemu.c",
  "sim/arm/kid.c", "sim/arm/thumbemu.c", "sim/arm/armdefs.h",
  "sim/arm/armopts.h", "sim/arm/dbg_cp.h", "sim/arm/dbg_rdi.h",
```

"sim/arm/parent.c", "sim/arm/armsupp.c", "sim/arm/armrdi.c",
"sim/arm/bag.c",
"sim/arm/armvirt.c", "sim/arm/main.c", "sim/arm/bag.h",
"sim/arm/communicate.c", "sim/arm/gdbhost.h", "sim/arm/armfpe.h",
"sim/arm/arminit.c",
"sim/common/cgen-fpu.c", "sim/common/cgen-fpu.h",
"sim/common/cgen-accfp.c",
"sim/mips/m16run.c", "sim/mips/sim-main.c",
"sim/moxie/moxie-gdb.dts",
Not a single file in sim/ppc/ appears to be copyright FSF :-(.
"sim/ppc/filter.h", "sim/ppc/gen-support.h", "sim/ppc/ld-insn.h",
"sim/ppc/hw_sem.c", "sim/ppc/hw_disk.c", "sim/ppc/idecode_branch.h",
"sim/ppc/sim-endian.h", "sim/ppc/table.c", "sim/ppc/hw_core.c",
"sim/ppc/gen-support.c", "sim/ppc/gen-semantics.h", "sim/ppc/cpu.h",
"sim/ppc/sim_callbacks.h", "sim/ppc/RUN", "sim/ppc/Makefile.in",
"sim/ppc/emul_chirp.c", "sim/ppc/hw_nvram.c", "sim/ppc/dc-test.01",
"sim/ppc/hw_phb.c", "sim/ppc/hw_eeprom.c", "sim/ppc/bits.h",
"sim/ppc/hw_vm.c", "sim/ppc/cap.h", "sim/ppc/os_emul.h",
"sim/ppc/options.h", "sim/ppc/gen-idecode.c", "sim/ppc/filter.c",
"sim/ppc/corefile-n.h", "sim/ppc/std-config.h", "sim/ppc/ld-decode.h",
"sim/ppc/filter_filename.h", "sim/ppc/hw_shm.c",
"sim/ppc/pk_disklabel.c", "sim/ppc/dc-simple", "sim/ppc/misc.h",
"sim/ppc/device_table.h", "sim/ppc/ld-insn.c", "sim/ppc/inline.c",
"sim/ppc/emul_bugapi.h", "sim/ppc/hw_cpu.h", "sim/ppc/debug.h",
"sim/ppc/hw_ide.c", "sim/ppc/debug.c", "sim/ppc/gen-itable.h",
"sim/ppc/interrupts.c", "sim/ppc/hw_glue.c", "sim/ppc/emul_unix.c",
"sim/ppc/sim_calls.c", "sim/ppc/dc-complex", "sim/ppc/ld-cache.c",
"sim/ppc/registers.h", "sim/ppc/dc-test.02", "sim/ppc/options.c",
"sim/ppc/igen.h", "sim/ppc/registers.c", "sim/ppc/device.h",
"sim/ppc/emul_chirp.h", "sim/ppc/hw_register.c", "sim/ppc/hw_init.c",
"sim/ppc/sim-endian-n.h", "sim/ppc/filter_filename.c",
"sim/ppc/bits.c", "sim/ppc/idecode_fields.h", "sim/ppc/hw_memory.c",
"sim/ppc/misc.c", "sim/ppc/double.c", "sim/ppc/psim.h",
"sim/ppc/hw_trace.c", "sim/ppc/emul_netbsd.h",
"sim/ppc/psim.c",
"sim/ppc/ppc-instructions", "sim/ppc/tree.h", "sim/ppc/README",
"sim/ppc/gen-icache.h", "sim/ppc/gen-model.h", "sim/ppc/ld-cache.h",
"sim/ppc/mon.c", "sim/ppc/corefile.h", "sim/ppc/vm.c",
"sim/ppc/INSTALL", "sim/ppc/gen-model.c", "sim/ppc/hw_cpu.c",
"sim/ppc/corefile.c", "sim/ppc/hw_opic.c", "sim/ppc/gen-icache.c",
"sim/ppc/events.h", "sim/ppc/os_emul.c", "sim/ppc/emul_generic.c",
"sim/ppc/main.c", "sim/ppc/hw_com.c", "sim/ppc/gen-semantics.c",
"sim/ppc/emul_bugapi.c", "sim/ppc/device.c", "sim/ppc/emul_generic.h",
"sim/ppc/tree.c", "sim/ppc/mon.h", "sim/ppc/interrupts.h",
"sim/ppc/cap.c", "sim/ppc/cpu.c", "sim/ppc/hw_phb.h",
"sim/ppc/device_table.c", "sim/ppc/lf.c", "sim/ppc/lf.c",
"sim/ppc/dc-stupid", "sim/ppc/hw_pal.c", "sim/ppc/ppc-spr-table",
"sim/ppc/emul_unix.h", "sim/ppc/words.h", "sim/ppc/basics.h",

```
  "sim/ppc/hw_htab.c", "sim/ppc/lf.h", "sim/ppc/ld-decode.c",
  "sim/ppc/sim-endian.c", "sim/ppc/gen-itable.c",
   "sim/ppc/idecode_expression.h", "sim/ppc/table.h", "sim/ppc/dgen.c",
  "sim/ppc/events.c", "sim/ppc/gen-idecode.h", "sim/ppc/emul_netbsd.c",
  "sim/ppc/igen.c", "sim/ppc/vm_n.h", "sim/ppc/vm.h",
  "sim/ppc/hw_iobus.c", "sim/ppc/inline.h",
  "sim/testsuite/sim/bfin/s21.s", "sim/testsuite/sim/mips/mips32-dsp2.s",
)

if __name__ == "__main__":
  main()
@ignore
@c Set file name and title for man page.
@setfilename gpl
@settitle GNU General Public License
@c man begin SEEALSO
gfdl(7), fsf-funding(7).
@c man end
@c man begin COPYRIGHT
Copyright @copyright{} 2007 Free Software Foundation, Inc. @url{http://fsf.org/}

Everyone is permitted to copy and distribute verbatim copies of this
license document, but changing it is not allowed.
@c man end
@end ignore
@node Copying
@c man begin DESCRIPTION
@appendix GNU GENERAL PUBLIC LICENSE
@c The GNU General Public License.
@center Version 3, 29 June 2007

@c This file is intended to be included within another document,
@c hence no sectioning command or @node.

@display
Copyright @copyright{} 2007 Free Software Foundation, Inc. @url{http://fsf.org/}

Everyone is permitted to copy and distribute verbatim copies of this
license document, but changing it is not allowed.
@end display

@heading Preamble

The GNU General Public License is a free, copyleft license for
software and other kinds of works.

The
```

licenses for most software and other practical works are designed
to take away your freedom to share and change the works. By contrast,
the GNU General Public License is intended to guarantee your freedom
to share and change all versions of a program---to make sure it remains
free software for all its users. We, the Free Software Foundation,
use the GNU General Public License for most of our software; it
applies also to any other work released this way by its authors. You
can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not
price. Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
them if you wish), that you receive source code or can get it if you
want it, that you can change the software or use pieces of it in new
free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you
these rights
or asking you to surrender the rights. Therefore, you
have certain responsibilities if you distribute copies of the
software, or if you modify it: responsibilities to respect the freedom
of others.

For example, if you distribute copies of such a program, whether
gratis or for a fee, you must pass on to the recipients the same
freedoms that you received. You must make sure that they, too,
receive or can get the source code. And you must show them these
terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps:
(1) assert copyright on the software, and (2) offer you this License
giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains
that there is no warranty for this free software. For both users' and
authors' sake, the GPL requires that modified versions be marked as
changed, so that their problems will not be attributed erroneously to
authors of previous
versions.

Some devices are designed to deny users access to install or run
modified versions of the software inside them, although the
manufacturer can do so. This is fundamentally incompatible with the
aim of protecting users' freedom to change the software. The
systematic pattern of such abuse occurs in the area of products for
individuals to use, which is precisely where it is most unacceptable.
Therefore, we have designed this version of the GPL to prohibit the
practice for those products. If such problems arise substantially in

other domains, we stand ready to extend this provision to those
domains in future versions of the GPL, as needed to protect the
freedom of users.

Finally, every program is threatened constantly by software patents.
States should not allow patents to restrict development and use of
software on general-purpose computers, but in those that do, we wish
to avoid the special danger that patents applied to a free program
could make it effectively proprietary.
To prevent this, the GPL
assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and
modification follow.

@heading TERMS AND CONDITIONS

@enumerate 0
@item Definitions.

``This License'' refers to version 3 of the GNU General Public License.

``Copyright'' also means copyright-like laws that apply to other kinds
of works, such as semiconductor masks.

``The Program'' refers to any copyrightable work licensed under this
License. Each licensee is addressed as ``you''. ``Licensees'' and
``recipients'' may be individuals or organizations.

To ``modify'' a work means to copy from or adapt all or part of the work
in a fashion requiring copyright permission, other than the making of
an exact copy. The resulting work is called a ``modified version'' of
the earlier work or a work ``based on'' the earlier work.

A ``covered work'' means either the unmodified Program or a work based
on the Program.

To ``propagate'' a
work means to do anything with it that, without
permission, would make you directly or secondarily liable for
infringement under applicable copyright law, except executing it on a
computer or modifying a private copy. Propagation includes copying,
distribution (with or without modification), making available to the
public, and in some countries other activities as well.

To ``convey'' a work means any kind of propagation that enables other
parties to make or receive copies. Mere interaction with a user
through a computer network, with no transfer of a copy, is not

conveying.

An interactive user interface displays ``Appropriate Legal Notices'' to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface
presents a list of user commands or options, such as a
menu, a prominent item in the list meets this criterion.

@item Source Code.

The ``source code'' for a work means the preferred form of the work for making modifications to it. ``Object code'' means any non-source form of a work.

A ``Standard Interface'' means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The ``System Libraries'' of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A ``Major Component'', in this context,
means a major essential component
(kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The ``Corresponding Source'' for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms

and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

@item Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively
for you, or provide you with
facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

@item Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to
forbid
circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against

the work's users, your or third parties' legal rights to forbid
circumvention of technological measures.

@item Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you
receive it, in any medium, provided that you conspicuously and
appropriately publish on each copy an appropriate copyright notice;
keep intact all notices stating that this License and any
non-permissive terms added in accord with section 7 apply to the code;
keep intact all notices of the absence of any warranty; and give all
recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey,
and you may offer support or warranty protection for a fee.

@item
Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to
produce it from the Program, in the form of source code under the
terms of section 4, provided that you also meet all of these
conditions:

@enumerate a
@item
The work must carry prominent notices stating that you modified it,
and giving a relevant date.

@item
The work must carry prominent notices stating that it is released
under this License and any conditions added under section 7. This
requirement modifies the requirement in section 4 to ``keep intact all
notices''.

@item
You must license the entire work, as a whole, under this License to
anyone who comes into possession of a copy. This License will
therefore apply, along with any applicable section 7 additional terms,
to the whole of the work, and all its parts, regardless of how they
are packaged. This License gives no permission to license the work in
any other way, but it does not invalidate such permission if
you have
separately received it.

@item
If the work has interactive user interfaces, each must display
Appropriate Legal Notices; however, if the Program has interactive

interfaces that do not display Appropriate Legal Notices, your work
need not make them do so.
@end enumerate

A compilation of a covered work with other separate and independent
works, which are not by their nature extensions of the covered work,
and which are not combined with it such as to form a larger program,
in or on a volume of a storage or distribution medium, is called an
``aggregate'' if the compilation and its resulting copyright are not
used to limit the access or legal rights of the compilation's users
beyond what the individual works permit. Inclusion of a covered work
in an aggregate does not cause this License to apply to the other
parts of the aggregate.

@item Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of
sections 4 and 5, provided that you also convey
 the machine-readable
Corresponding Source under the terms of this License, in one of these
ways:

@enumerate a
@item
Convey the object code in, or embodied in, a physical product
(including a physical distribution medium), accompanied by the
Corresponding Source fixed on a durable physical medium customarily
used for software interchange.

@item
Convey the object code in, or embodied in, a physical product
(including a physical distribution medium), accompanied by a written
offer, valid for at least three years and valid for as long as you
offer spare parts or customer support for that product model, to give
anyone who possesses the object code either (1) a copy of the
Corresponding Source for all the software in the product that is
covered by this License, on a durable physical medium customarily used
for software interchange, for a price no more than your reasonable
cost of physically performing this conveying of source, or (2) access
to copy the Corresponding Source from a network
 server at no charge.

@item
Convey individual copies of the object code with a copy of the written
offer to provide the Corresponding Source. This alternative is
allowed only occasionally and noncommercially, and only if you
received the object code with such an offer, in accord with subsection
6b.

@item
Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to
ensure that it is available for as long as needed to
satisfy these requirements.

@item
Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

@end enumerate

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A ``User Product'' is either (1) a ``consumer product'', which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, ``normally used'' refers to a typical or common use of that class of product, regardless of
the status of the particular user or of the way
in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

``Installation Information'' for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of

the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User
Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this
section must be in a format that is publicly
documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

@item Additional Terms.

``Additional permissions'' are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain
cases when you modify the work.) You may place
additional permissions on material, added by you to a covered work,

for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

@enumerate a
@item
Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

@item
Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

@item
Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

@item
Limiting the use for publicity purposes of names of licensors or authors of the material; or

@item
Declining
to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

@item
Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.
@end enumerate

All other non-permissive additional terms are considered ``further restrictions'' within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing

or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

@item Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder
fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

@item Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission
to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or

modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

@item Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An ``entity transaction'' is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy
of the work also receives whatever
licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

@item Patents.

A ``contributor'' is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's ``contributor version''.

A
contributor's ``essential patent claims'' are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, ``control'' includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free

patent license under the contributor's essential patent claims, to
make, use, sell, offer for sale, import and otherwise run, modify and
propagate the contents of its contributor version.

In the following three paragraphs, a ``patent license" is any express
agreement or commitment, however denominated, not to enforce a patent
(such as an express permission to practice
a patent or covenant not to
sue for patent infringement). To ``grant" such a patent license to a
party means to make such an agreement or commitment not to enforce a
patent against the party.

If you convey a covered work, knowingly relying on a patent license,
and the Corresponding Source of the work is not available for anyone
to copy, free of charge and under the terms of this License, through a
publicly available network server or other readily accessible means,
then you must either (1) cause the Corresponding Source to be so
available, or (2) arrange to deprive yourself of the benefit of the
patent license for this particular work, or (3) arrange, in a manner
consistent with the requirements of this License, to extend the patent
license to downstream recipients. ``Knowingly relying" means you have
actual knowledge that, but for the patent license, your conveying the
covered work in a country, or your recipient's use of the covered work
in a country, would infringe one or more
identifiable patents in that
country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or
arrangement, you convey, or propagate by procuring conveyance of, a
covered work, and grant a patent license to some of the parties
receiving the covered work authorizing them to use, propagate, modify
or convey a specific copy of the covered work, then the patent license
you grant is automatically extended to all recipients of the covered
work and works based on it.

A patent license is ``discriminatory" if it does not include within the
scope of its coverage, prohibits the exercise of, or is conditioned on
the non-exercise of one or more of the rights that are specifically
granted under this License. You may not convey a covered work if you
are a party to an arrangement with a third party that is in the
business of distributing software, under which you make payment to the
third party based on the extent of your activity of conveying the
work,
and under which the third party grants, to any of the parties
who would receive the covered work from you, a discriminatory patent
license (a) in connection with copies of the covered work conveyed by
you (or copies made from those copies), or (b) primarily for and in
connection with specific products or compilations that contain the

covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

@item No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent
obligations, then as a
consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

@item Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

@item Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of
the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License ``or any later version'' applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions
of the GNU General Public License can be used, that proxy's public
statement of acceptance of a version permanently authorizes you to
choose that version for the Program.

Later license versions may give you additional or different
permissions.
However, no additional obligations are imposed on any
author or copyright holder as a result of your choosing to follow a
later version.

@item Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM ``AS IS'' WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

@item Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL,
INCIDENTAL OR CONSEQUENTIAL DAMAGES
ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

@item Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided
above cannot be given local legal effect according to their terms,
reviewing courts shall apply local law that most closely approximates
an absolute waiver of all civil liability in connection with the
Program, unless a warranty or assumption of liability accompanies a
copy of the Program in return for a fee.

@end enumerate

@heading END OF TERMS AND CONDITIONS

@heading How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest
possible use to the public, the
best way to achieve this is to make it
free software which everyone can redistribute and change under these
terms.

To do so, attach the following notices to the program. It is safest
to attach them to the start of each source file to most effectively
state the exclusion of warranty; and each file should have at least
the ``copyright'' line and a pointer to where the full notice is found.

@smallexample
@var{one line to give the program's name and a brief idea of what it does.}
Copyright (C) @var{year} @var{name of author}

This program is free software: you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation, either version 3 of the License, or (at
your option) any later version.

This program is distributed in the hope that it will be useful, but
WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
General Public License for more details.

You
should have received a copy of the GNU General Public License
along with this program. If not, see @url{http://www.gnu.org/licenses/}.
@end smallexample

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

@smallexample
@var{program} Copyright (C) @var{year} @var{name of author}
This program comes with ABSOLUTELY NO WARRANTY; for details type @samp{show w}.
This is free software, and you are welcome to redistribute it
under certain conditions; type @samp{show c} for details.
@end smallexample

The hypothetical commands @samp{show w} and @samp{show c} should show
the appropriate parts of the General Public License. Of course, your

program's commands might be different; for a GUI interface, you would
use an ``about box".

You should also get your employer (if you work as a programmer) or school,
if any, to sign a ``copyright disclaimer"
 for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
@url{http://www.gnu.org/licenses/}.

The GNU General Public License does not permit incorporating your
program into proprietary programs. If your program is a subroutine
library, you may consider it more useful to permit linking proprietary
applications with the library. If this is what you want to do, use
the GNU Lesser General Public License instead of this License. But
first, please read @url{http://www.gnu.org/philosophy/why-not-lgpl.html}.
@c man end
   GNU LIBRARY GENERAL PUBLIC LICENSE
      Version 2, June 1991

Copyright (C) 1991 Free Software Foundation, Inc.
            675 Mass Ave, Cambridge, MA 02139, USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the library GPL. It is
numbered 2 because it goes with version 2 of the ordinary GPL.]

      Preamble

 The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
Licenses are intended to guarantee your freedom to share and change
free software--to make sure the software is free for all its users.

 This license, the Library General Public License, applies to some
specially designated Free Software Foundation software, and to any
other libraries whose authors decide to use it. You can use it for
your libraries, too.

 When we speak of free software, we are referring to freedom,
 not
price. Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

 To protect your rights, we need to make restrictions that forbid

anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate to certain responsibilities for you if
you distribute copies of the library, or if you modify it.

For example, if you distribute copies of the library, whether gratis
or for a fee, you must give the recipients all the rights that we gave
you. You must make sure that they, too, receive or can get the source
code. If you link a program with the library, you must provide
complete object files to the recipients so that they can relink them
with the library, after making changes
to the library and recompiling
it. And you must show them these terms so they know their rights.

Our method of protecting your rights has two steps: (1) copyright
the library, and (2) offer you this license which gives you legal
permission to copy, distribute and/or modify the library.

Also, for each distributor's protection, we want to make certain
that everyone understands that there is no warranty for this free
library. If the library is modified by someone else and passed on, we
want its recipients to know that what they have is not the original
version, so that any problems introduced by others will not reflect on
the original authors' reputations.

Finally, any free program is threatened constantly by software
patents. We wish to avoid the danger that companies distributing free
software will individually obtain patent licenses, thus in effect
transforming the program into proprietary software. To prevent this,
we have made it clear that any patent must be licensed
for everyone's
free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary
GNU General Public License, which was designed for utility programs. This
license, the GNU Library General Public License, applies to certain
designated libraries. This license is quite different from the ordinary
one; be sure to read it in full, and don't assume that anything in it is
the same as in the ordinary license.

The reason we have a separate public license for some libraries is that
they blur the distinction we usually make between modifying or adding to a
program and simply using it. Linking a program with a library, without
changing the library, is in some sense simply using the library, and is
analogous to running a utility program or application program. However, in
a textual and legal sense, the linked executable is a combined work, a
derivative of the original library, and the ordinary General Public License
treats it as such.

Because
of this blurred distinction, using the ordinary General
Public License for libraries did not effectively promote software
sharing, because most developers did not use the libraries. We
concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the
users of those programs of all benefit from the free status of the
libraries themselves. This Library General Public License is intended to
permit developers of non-free programs to use free libraries, while
preserving your freedom as a user of such programs to change the free
libraries that are incorporated in them. (We have not seen how to achieve
this as regards changes in header files, but we have achieved it as regards
changes in the actual functions of the Library.) The hope is that this
will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and
modification follow. Pay close attention to the difference
between a
"work based on the library" and a "work that uses the library". The
former contains code derived from the library, while the latter only
works together with the library.

Note that it is possible for a library to be covered by the ordinary
General Public License rather than by this special one.

GNU LIBRARY GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which
contains a notice placed by the copyright holder or other authorized
party saying it may be distributed under the terms of this Library
General Public License (also called "this License"). Each licensee is
addressed as "you".

A "library" means a collection of software functions and/or data
prepared so as to be conveniently linked with application programs
(which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work
which has been distributed
under these terms. A "work based on the
Library" means either the Library or any derivative work under
copyright law: that is to say, a work containing the Library or a
portion of it, either verbatim or with modifications and/or translated
straightforwardly into another language. (Hereinafter, translation is
included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also compile or link a "work that uses the Library" with the Library to produce a

work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

c) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

d) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute
the Library at all. For example, if a patent
license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system;
it is up to the author/donor to decide if he or she is willing
to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Library General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each

version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS
LICENSED FREE OF CHARGE, THERE IS NO
WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES
SUSTAINED BY YOU OR THIRD PARTIES OR A
FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Appendix: How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that

everyone can redistribute and change. You can do so by permitting
redistribution under these terms (or, alternatively, under the terms of the
ordinary General Public License).

 To apply these terms, attach the following notices to the library. It is
safest to attach them to the start of each source file to most effectively
convey the exclusion of warranty; and each file should have at least the
"copyright" line and a pointer to where the full notice is found.

  <one line to give the library's name and a brief idea of what it does.>
  Copyright (C) <year>
 <name of author>

  This library is free software; you can redistribute it and/or
  modify it under the terms of the GNU Library General Public
  License as published by the Free Software Foundation; either
  version 2 of the License, or (at your option) any later version.

  This library is distributed in the hope that it will be useful,
  but WITHOUT ANY WARRANTY; without even the implied warranty of
  MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
  Library General Public License for more details.

  You should have received a copy of the GNU Library General Public
  License along with this library; if not, write to the Free
  Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the library, if
necessary. Here is a sample; alter
 the names:

 Yoyodyne, Inc., hereby disclaims all copyright interest in the
 library `Frob' (a library for tweaking knobs) written by James Random Hacker.

 <signature of Ty Coon>, 1 April 1990
 Ty Coon, President of Vice

That's all there is to it!

1.69 net-tools 1.60

1.69.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
675 Mass Ave, Cambridge, MA 02139, USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it. (Some other Free Software Foundation software is covered by
the GNU Library General Public License instead.) You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price. Our General Public Licenses are designed
to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid
anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate to certain responsibilities for you if you
distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether
gratis or for a fee, you must give the recipients all the rights that
you have. You must make sure that they, too, receive or can get the
source code. And you must show them these terms so they know their
rights.

We protect your rights with two steps: (1) copyright the software, and
(2) offer you this license which gives you legal permission to copy,
distribute
and/or modify the software.

Also, for each author's protection and ours, we want to make certain
that everyone understands that there is no warranty for this free
software. If the software is modified by someone else and passed on, we

want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and

distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole
or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably
considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it,
under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are

prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6.
Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free
redistribution of the Program by
all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through
any other system and a licensee cannot
impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in
certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Program under this License
may add an explicit geographical distribution limitation excluding
those countries, so that distribution is permitted only in or among
countries not thus excluded. In such case, this License incorporates
the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions
of the General Public License from time to time. Such new versions will
be similar in spirit to the present version, but may differ in detail to
address new problems or concerns.

Each version is given a distinguishing version number. If the Program
specifies a version number
of this License which applies to it and "any
later version", you have the option of following the terms and conditions
either of that version or of any later version published by the Free
Software Foundation. If the Program does not specify a version number of
this License, you may choose any version ever published by the Free Software
Foundation.

10. If you wish to incorporate parts of the Program into other free
programs whose distribution conditions are different, write to the author
to ask for permission. For software which is copyrighted by the Free
Software Foundation, write to the Free Software Foundation; we sometimes
make exceptions for this. Our decision will be guided by the two goals
of preserving the free status of all derivatives of our free software and
of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY
FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE
LAW. EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES
PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED
OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS
TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE
PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING,
REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING
WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR
REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES,
INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING

OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS),
EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Appendix: How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) 19yy <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19yy name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c'
should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this is what you want to do, use the GNU Library General
Public License instead of this License.

1.70 libnss-mdns 0.10

1.70.1 Available under license :

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts
as the successor of the GNU Library Public License, version 2, hence
the version number 2.1.]

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
Licenses are intended to guarantee your freedom to share and change
free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some
specially designated software packages--typically libraries--of the

Free Software Foundation and other authors who decide
to use it. You
can use it too, but we suggest you first think carefully about whether
this license or the ordinary General Public License is the better
strategy to use in any particular case, based on the explanations
below.

When we speak of free software, we are referring to freedom of use,
not price. Our General Public Licenses are designed to make sure that
you have the freedom to distribute copies of free software (and charge
for this service if you wish); that you receive source code or can get
it if you want it; that you can change the software and use pieces of
it in new free programs; and that you are informed that you can do
these things.

To protect your rights, we need to make restrictions that forbid
distributors to deny you these rights or to ask you to surrender these
rights. These restrictions translate to certain responsibilities for
you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether
gratis
or for a fee, you must give the recipients all the rights that we gave
you. You must make sure that they, too, receive or can get the source
code. If you link other code with the library, you must provide
complete object files to the recipients, so that they can relink them
with the library after making changes to the library and recompiling
it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the
library, and (2) we offer you this license, which gives you legal
permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that
there is no warranty for the free library. Also, if the library is
modified by someone else and passed on, the recipients should know
that what they have is not the original version, so that the original
author's reputation will not be affected by problems that might be
introduced by others.

Finally, software
patents pose a constant threat to the existence of
any free program. We wish to make sure that a company cannot
effectively restrict the users of a free program by obtaining a
restrictive license from a patent holder. Therefore, we insist that
any patent license obtained for a version of the library must be
consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits
such linking only if the
entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the
free library to free
software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The

former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to

exercise the right to control the distribution of derivative or
collective works based on the Library.

In addition, mere aggregation of another work not based on the Library
with the Library (or with a work based on the Library) on a volume of
a storage or distribution medium does not bring the other work under
the scope of this License.

3. You may opt to apply the terms of the ordinary
GNU General Public
License instead of this License to a given copy of the Library. To do
this, you must alter all the notices that refer to this License, so
that they refer to the ordinary GNU General Public License, version 2,
instead of to this License. (If a newer version than version 2 of the
ordinary GNU General Public License has appeared, then you can specify
that version instead if you wish.) Do not make any other change in
these notices.

Once this change is made in a given copy, it is irreversible for
that copy, so the ordinary GNU General Public License applies to all
subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of
the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or
derivative of it, under Section 2) in object code or executable form
under the terms of Sections 1 and 2 above provided that you accompany
it with the complete corresponding
machine-readable source code, which
must be distributed under the terms of Sections 1 and 2 above on a
medium customarily used for software interchange.

If distribution of object code is made by offering access to copy
from a designated place, then offering equivalent access to copy the
source code from the same place satisfies the requirement to
distribute the source code, even though third parties are not
compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the
Library, but is designed to work with the Library by being compiled or
linked with it, is called a "work that uses the Library". Such a
work, in isolation, is not a derivative work of the Library, and
therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library
creates an executable that is a derivative of the Library (because it
contains portions of the Library), rather than a "work that uses

the
library". The executable is therefore covered by this License.
Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object
code for the work under the terms of Section 6.
Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the
work with the complete corresponding
machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood

that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly
with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally
distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to

refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system
which is
implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish
revised and/or new
versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free

Software Foundation; we sometimes make exceptions for this. Our decision will
be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU
FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively
convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or
modify it under the terms of the GNU Lesser General Public
License as published by the Free Software Foundation; either
version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public
License along with this library; if not, write to the Free Software
Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301
USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or
your school, if any, to sign a "copyright disclaimer" for the library,
if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the
library `Frob' (a library for tweaking knobs) written by James
Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

1.71 libgpg-error 1.24

1.71.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your

freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed
to make sure that you
have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute
and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work
which contains
a notice placed by the copyright holder saying it may be distributed
under the terms of this General Public License. The "Program", below,
refers to any such program or work, and a "work based on the Program"
means either the Program or any derivative work under copyright law:
that is to say, a work containing the Program or a portion of it,
either verbatim or with modifications and/or translated into another
language. (Hereinafter, translation is included without limitation in
the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not
covered by this License; they are outside its scope. The act of
running the Program is not restricted, and the output from the Program
is covered only if its contents constitute a work based on the
Program (independent of having been made by running the Program).
Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim
copies of the Program's
source code as you receive it, in any medium, provided that you
conspicuously and appropriately publish on each copy an appropriate
copyright notice and disclaimer of warranty; keep intact all the
notices that refer to this License and to the absence of any warranty;
and give any other recipients of the Program a copy of this License
along with the Program.

You may charge a fee for the physical act of transferring a copy, and
you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion
of it, thus forming a work based on the Program, and copy and
distribute such modifications or work under the terms of Section 1
above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices
stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in

whole or in part contains or is derived from the Program or any
part thereof, to be licensed as a whole at no charge to all third
parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6.
Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein.

You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to

address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version
number of this License which applies to it and "any
later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE
LAW. EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS),
EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest

possible use to the public, the best way to achieve this is to make it
free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest
to attach them to the start of each source file to most effectively
convey the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation; either version 2 of the
License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands
`show w' and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid

distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no

charge to all third parties under the terms
of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably
considered independent and separate works in
themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary
GNU General Public
License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in

these notices.

Once this change is made in a given copy, it is irreversible for
that copy, so the ordinary GNU General Public License applies to all
subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of
the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or
derivative of it, under Section 2) in object code or executable form
under the terms of Sections 1 and 2 above provided that you accompany
it with the complete corresponding
machine-readable source code, which
must be distributed under the terms of Sections 1 and 2 above on a
medium customarily used for software interchange.

If distribution of object code is made by offering access to copy
from a designated place, then offering equivalent access to copy the
source code from the same place satisfies the requirement to
distribute the source code, even though third parties are not
compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the
Library, but is designed to work with the Library by being compiled or
linked with it, is called a "work that uses the Library". Such a
work, in isolation, is not a derivative work of the Library, and
therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library
creates an executable that is a derivative of the Library (because it
contains portions of the Library), rather than a "work that uses
the
library". The executable is therefore covered by this License.
Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file
that is part of the Library, the object code for the work may be a
derivative work of the Library even though the source code is not.
Whether this is true is especially significant if the work can be
linked without the Library, or if the work is itself a library. The
threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data
structure layouts and accessors, and small macros and small inline
functions (ten lines or less in length), then the use of the object
file is unrestricted, regardless of whether it is legally a derivative
work. (Executables containing this object code plus portions of the

Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object
code for the work under the terms of Section 6.
Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the
work with the complete corresponding
machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly
with a modified version of the library, if
the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of

performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally
distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any
other library
facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses

terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing

to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME

THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301

USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or
your school, if any, to sign a "copyright disclaimer" for the library,
if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the
library `Frob' (a library for tweaking knobs) written by James
Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

1.72 zeromq 4.1.5

1.72.1 Available under license :

wepoll - epoll for Windows
https://github.com/piscisaureus/wepoll

Copyright 2012-2018, Bert Belder <bertbelder@gmail.com>
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are
met:

* Redistributions of source code must retain the above copyright
  notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT
OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY,
 OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT

(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

GNU LESSER GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and the "GNU GPL" refers to version 3 of the GNU General Public License.

"The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An "Application" is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying
Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters,
data structure
layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license

document.

c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based

on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

SPECIAL EXCEPTION GRANTED BY COPYRIGHT HOLDERS

As a special exception, copyright holders give you permission to link this library with independent modules to produce an executable, regardless of the license terms of these independent modules, and to copy and distribute the resulting executable under terms of your choice, provided that you also meet, for each linked independent module, the terms and conditions of the license of that module. An independent module is a module which is not derived from or based on this library. If you modify this library, you must extend this exception to your version of the library.

Note: this exception relieves you of any obligations under sections 4 and 5 of this license, and section 6 of the GNU General Public License.

The MIT License (MIT)

Copyright (c) <year> 2007-14 Mike Karlesky, Mark VanderVoord, Greg Williams

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT,
TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for
software and other kinds of works.

The licenses for most software and other practical works are designed
to take away your freedom to share and change the works. By contrast,
the GNU General Public License is intended to guarantee your freedom to
share and change all versions of a program--to make sure it remains free
software for all its users. We, the Free Software Foundation, use the
GNU General Public License for most of our software; it applies also to
any other work released this way by its authors. You can apply it to
your programs, too.

When we speak of free software, we are referring to
freedom, not
price. Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
them if you wish), that you receive source code or can get it if you

want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1)
assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains,
we
stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed;
section 10
makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately
publish on each copy an appropriate copyright notice;
keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code;
keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium

customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation

into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization
keys, or other information required to install
and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed
in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this

License by making exceptions from one or more of its conditions.
Additional permissions that are applicable to the
entire Program shall
be treated as though they were included in this License, to the extent
that they are valid under applicable law. If additional permissions
apply only to part of the Program, that part may be used separately
under those permissions, but the entire Program remains governed by
this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option
remove any additional permissions from that copy, or from any part of
it. (Additional permissions may be written to require their own
removal in certain cases when you modify the work.) You may place
additional permissions on material, added by you to a covered work,
for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you
add to a covered work, you may (if authorized by the copyright holders of
that material) supplement the terms of this License with terms:

a) Disclaiming warranty
or limiting liability differently from the
terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or
author attributions in that material or in the Appropriate Legal
Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or
requiring that modified versions of such material be marked in
reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or
authors of the material; or

e) Declining to grant rights under trademark law for use of some
trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that
material by anyone who conveys the material (or modified versions of
it) with contractual assumptions of liability to the recipient, for
any liability that these contractual assumptions directly impose on

those licensors and authors.

All other non-permissive additional terms are considered "further
restrictions" within the meaning of section 10. If the Program as you
received it, or any part of it, contains a notice stating that it is

governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights
granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor

version. For
purposes of this definition, "control" includes the right to grant
patent sublicenses in a manner consistent with the requirements of
this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free
patent license under the contributor's essential patent claims, to
make, use, sell, offer for sale, import and otherwise run, modify and
propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express
agreement or commitment, however denominated, not to enforce a patent
(such as an express permission to practice a patent or covenant not to
sue for patent infringement). To "grant" such a patent license to a
party means to make such an agreement or commitment not to enforce a
patent against the party.

If you convey a covered work, knowingly relying on a patent license,
and the Corresponding Source of the work is not available for anyone
to copy, free of charge and under the terms of this
License, through a
publicly available network server or other readily accessible means,
then you must either (1) cause the Corresponding Source to be so
available, or (2) arrange to deprive yourself of the benefit of the
patent license for this particular work, or (3) arrange, in a manner
consistent with the requirements of this License, to extend the patent
license to downstream recipients. "Knowingly relying" means you have
actual knowledge that, but for the patent license, your conveying the
covered work in a country, or your recipient's use of the covered work
in a country, would infringe one or more identifiable patents in that
country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or
arrangement, you convey, or propagate by procuring conveyance of, a
covered work, and grant a patent license to some of the parties
receiving the covered work authorizing them to use, propagate, modify
or convey a specific copy of the covered
work, then the patent license
you grant is automatically extended to all recipients of the covered
work and works based on it.

A patent license is "discriminatory" if it does not include within
the scope of its coverage, prohibits the exercise of, or is
conditioned on the non-exercise of one or more of the rights that are
specifically granted under this License. You may not convey a covered
work if you are a party to an arrangement with a third party that is
in the business of distributing software, under which you make payment
to the third party based on the extent of your activity of conveying

the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement,
or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it,

you have the
option of following the terms and conditions either of that numbered
version or of any later version published by the Free Software
Foundation. If the Program does not specify a version number of the
GNU General Public License, you may choose any version ever published
by the Free Software Foundation.

If the Program specifies that a proxy can decide which future
versions of the GNU General Public License can be used, that proxy's
public statement of acceptance of a version permanently authorizes you
to choose that version for the Program.

Later license versions may give you additional or different
permissions. However, no additional obligations are imposed on any
author or copyright holder as a result of your choosing to follow a
later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY
APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT
HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS"
WITHOUT WARRANTY
OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM
IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF
ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING
WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS
THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY
GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE
USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF
DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD
PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS),
EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF
SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided
above cannot be given local legal effect according to their terms,
reviewing courts shall apply local law that most closely approximates
an absolute waiver of all civil liability in connection with the

Program, unless a warranty or assumption of liability accompanies a
copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest
possible use to the public, the best way to achieve this is to make it
free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest
to attach them to the start of each source file to most effectively
state the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where
the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation, either version 3 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>
This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school,

if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what you want to
do, use the GNU Lesser General
Public License instead of this License. But first, please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.

1.73 sqlite 3.14.1

1.73.1 Available under license :

The author disclaims copyright to this source code. In place of
a legal notice, here is a blessing:

May you do good and not evil.
May you find forgiveness for yourself and forgive others.
May you share freely, never taking more than you give.

1.74 libxml 2.9.4

1.74.1 Available under license :

Except where otherwise noted in the source code (e.g. the files hash.c,
list.c and the trio files, which are covered by a similar licence but
with different Copyright notices) all the files are:

Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is fur-
nished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FIT-
NESS FOR A PARTICULAR PURPOSE
AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER

LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

1.75 pixman 0.34.0

1.75.1 Available under license :

The following is the MIT license, agreed upon by most contributors.
Copyright holders of new code should use this license statement where
possible. They may also add themselves to the list below.

/*
* Copyright 1987, 1988, 1989, 1998 The Open Group
* Copyright 1987, 1988, 1989 Digital Equipment Corporation
* Copyright 1999, 2004, 2008 Keith Packard
* Copyright 2000 SuSE, Inc.
* Copyright 2000 Keith Packard, member of The XFree86 Project, Inc.
* Copyright 2004, 2005, 2007, 2008, 2009, 2010 Red Hat, Inc.
* Copyright 2004 Nicholas Miell
* Copyright 2005 Lars Knoll & Zack Rusin, Trolltech
* Copyright 2005 Trolltech AS
* Copyright 2007 Luca Barbato
* Copyright 2008 Aaron Plattner, NVIDIA Corporation
* Copyright 2008 Rodrigo Kumpera
* Copyright 2008 Andr Tupinamb
* Copyright 2008 Mozilla Corporation
* Copyright 2008 Frederic Plourde
* Copyright 2009, Oracle and/or its affiliates. All rights reserved.
* Copyright 2009, 2010 Nokia Corporation
*
* Permission is hereby granted,
 free of charge, to any person obtaining a
* copy of this software and associated documentation files (the "Software"),
* to deal in the Software without restriction, including without limitation
* the rights to use, copy, modify, merge, publish, distribute, sublicense,
* and/or sell copies of the Software, and to permit persons to whom the
* Software is furnished to do so, subject to the following conditions:
*
* The above copyright notice and this permission notice (including the next
* paragraph) shall be included in all copies or substantial portions of the
* Software.
*
* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
* IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
* FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL
* THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
* LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING

* FROM, OUT OF OR IN
CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER
* DEALINGS IN THE SOFTWARE.
*/

1.76 libnih 1.0.3

1.76.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it. (Some other Free Software Foundation software is covered by
the GNU Lesser General Public License instead.) You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price. Our General Public Licenses are designed
to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid
anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate to certain responsibilities for you if you
distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether
gratis or for a fee, you must give the recipients all the rights that
you have. You must make sure that they, too, receive or can get the
source code. And you must show them these terms so they know their
rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute
and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which
contains
a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies
of the Program's
source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty;

and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole
or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered
independent and separate works in
themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program

with the Program (or with a work based on the Program) on a volume of
a storage or distribution medium does not bring the other work under
the scope of this License.

3. You may copy and distribute the Program (or a work based
on it,
under Section 2) in object code or executable form under the terms of
Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable
source code, which must be distributed under the terms of Sections
1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three
years, to give any third party, for a charge no more than your
cost of physically performing source distribution, a complete
machine-readable copy of the corresponding source code, to be
distributed under the terms of Sections 1 and 2 above on a medium
customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer
to distribute corresponding source code. (This alternative is
allowed only for noncommercial distribution and only if you
received the program in object code or
executable form with such
an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for
making modifications to it. For an executable work, complete source
code means all the source code for all modules it contains, plus any
associated interface definition files, plus the scripts used to
control compilation and installation of the executable. However, as a
special exception, the source code distributed need not include
anything that is normally distributed (in either source or binary
form) with the major components (compiler, kernel, and so on) of the
operating system on which the executable runs, unless that component
itself accompanies the executable.

If distribution of executable or object code is made by offering
access to copy from a designated place, then offering equivalent
access to copy the source code from the same place counts as
distribution of the source code, even though third parties are not
compelled to copy the
source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program
except as expressly provided under this License. Any attempt
otherwise to copy, modify, sublicense or distribute the Program is

void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each
time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution
of the Program by
all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed

through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS

TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN
IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

```
Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.
```

The hypothetical commands `show w'
and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

```
Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice
```

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this is what you want to do, use the GNU Lesser General
Public License instead of this License.

1.77 gmp 6.1.1

1.77.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This

General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price.

Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which
gives you legal permission to copy,
distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a

notice that there is no warranty (or else, saying that you provide
a warranty) and that users may redistribute the program under
these conditions, and telling the user how to view a copy of this
License. (Exception: if the Program itself is interactive but
does not normally print such an announcement, your work based on
the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If
identifiable sections of that work
are not derived from the Program,
and can be reasonably considered independent and separate works in
themselves, then this License, and its terms, do not apply to those
sections when you distribute them as separate works. But when you
distribute the same sections as part of a whole which is a work based
on the Program, the distribution of the whole must be on the terms of
this License, whose permissions for other licensees extend to the
entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest
your rights to work written entirely by you; rather, the intent is to
exercise the right to control the distribution of derivative or
collective works based on the Program.

In addition, mere aggregation of another work not based on the Program
with the Program (or with a work based on the Program) on a volume of
a storage or distribution medium does not bring the other work under
the scope of this License.

3. You may copy and distribute the Program (or a work based on it,
under Section 2) in object code or executable form under the terms of
Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable
source code, which must be distributed under the terms of Sections
1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three
years, to give any third party, for a charge no more than your
cost of physically performing source distribution, a complete
machine-readable copy of the corresponding source code, to be
distributed under the terms of Sections 1 and 2 above on a medium
customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer
to distribute corresponding source code. (This alternative is
allowed only for noncommercial distribution
and only if you
received the program in object code or executable form with such

an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source
code, even though third parties are not
compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing
or modifying
the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues),

conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any

later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively

convey the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where the full notice is found.

  <one line to give the program's name and a brief idea of what it does.>
  Copyright (C) <year> <name of author>

  This program is free software; you can redistribute it and/or modify
  it under the terms of the GNU
General Public License as published by
  the Free Software Foundation; either version 2 of the License, or
  (at your option) any later version.

  This program is distributed in the hope that it will be useful,
  but WITHOUT ANY WARRANTY; without even the implied warranty of
  MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
  GNU General Public License for more details.

  You should have received a copy of the GNU General Public License along
  with this program; if not, write to the Free Software Foundation, Inc.,
  51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

  Gnomovision version 69, Copyright (C) year name of author
  Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
  This is free software, and you are welcome to redistribute
it
  under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

 Yoyodyne, Inc., hereby disclaims all copyright interest in the program
 `Gnomovision' (which makes passes at compilers) written by James Hacker.

 <signature of Ty Coon>, 1 April 1989
 Ty Coon, President of Vice

This General Public License does not permit incorporating your program into

proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this
is what you want to do, use the GNU Lesser General
Public License instead of this License.

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for
software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to
freedom, not
price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps:
(1)

assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand
ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees"
and
"recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the

earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately
publish on each copy an appropriate copyright notice;
keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This

License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the

written offer to provide the Corresponding Source. This
alternative is allowed only occasionally and noncommercially, and
only if you received the object code with such an offer, in accord
with subsection 6b.

d) Convey the object code by offering access from a designated
place (gratis or for a charge), and offer equivalent access to the
Corresponding Source in
the same way through the same place at no
further charge. You need not require recipients to copy the
Corresponding Source along with the object code. If the place to
copy the object code is a network server, the Corresponding Source
may be on a different server (operated by you or a third party)
that supports equivalent copying facilities, provided you maintain
clear directions next to the object code saying where to find the
Corresponding Source. Regardless of what server hosts the
Corresponding Source, you remain obligated to ensure that it is
available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided
you inform other peers where the object code and Corresponding
Source of the work are being offered to the general public at no
charge under subsection 6d.

A separable portion of the object code, whose source code is excluded
from the Corresponding Source
as a System Library, need not be
included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any
tangible personal property which is normally used for personal, family,
or household purposes, or (2) anything designed or sold for incorporation
into a dwelling. In determining whether a product is a consumer product,
doubtful cases shall be resolved in favor of coverage. For a particular
product received by a particular user, "normally used" refers to a
typical or common use of that class of product, regardless of the status
of the particular user or of the way in which the particular user
actually uses, or expects or is expected to use, the product. A product
is a consumer product regardless of whether the product has substantial
commercial, industrial or non-consumer uses, unless such uses represent
the only significant mode of use of the product.

"Installation Information" for a User Product means any methods,
procedures, authorization
keys, or other information required to install
and execute modified versions of a covered work in that User Product from
a modified version of its Corresponding Source. The information must
suffice to ensure that the continued functioning of the modified object

code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in
ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the
entire Program shall
be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above

requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright
holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible

for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights
granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For
purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a

patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the
option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY
OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17.
Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where
the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation, either version 3 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>
This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what you want to
do, use the GNU Lesser General
Public License instead of this License. But first, please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.
GNU LESSER GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies

of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and the "GNU GPL" refers to version 3 of the GNU General Public License.

"The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An "Application" is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the

facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for

them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1)
assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand
ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your

rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed;
section 10
makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately
publish on each copy an appropriate copyright notice;
keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the

Corresponding Source fixed on a durable physical medium
customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product
(including a physical distribution medium), accompanied by a
written offer, valid for at least three years
and valid for as
long as you offer spare parts or customer support for that product
model, to give anyone who possesses the object code either (1) a
copy of the Corresponding Source for all the software in the
product that is covered by this License, on a durable physical
medium customarily used for software interchange, for a price no
more than your reasonable cost of physically performing this
conveying of source, or (2) access to copy the
Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the
written offer to provide the Corresponding Source. This
alternative is allowed only occasionally and noncommercially, and
only if you received the object code with such an offer, in accord
with subsection 6b.

d) Convey the object code by offering access from a designated
place (gratis or for a charge), and offer equivalent access to the
Corresponding Source in
the same way through the same place at no
further charge. You need not require recipients to copy the
Corresponding Source along with the object code. If the place to
copy the object code is a network server, the Corresponding Source
may be on a different server (operated by you or a third party)
that supports equivalent copying facilities, provided you maintain
clear directions next to the object code saying where to find the
Corresponding Source. Regardless of what server hosts the
Corresponding Source, you remain obligated to ensure that it is
available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided
you inform other peers where the object code and Corresponding
Source of the work are being offered to the general public at no
charge under subsection 6d.

A separable portion of the object code, whose source code is excluded
from the Corresponding Source
as a System Library, need not be
included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any
tangible personal property which is normally used for personal, family,

or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you

received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above
requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright
holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights
granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a

consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment

to the third party based on the extent of your activity of conveying
the work, and under which the third party grants, to any of the
parties who would receive the covered work from you, a discriminatory
patent license (a) in connection with copies of the covered work
conveyed by you (or copies made from those copies), or (b) primarily
for and in connection with specific products or compilations that
contain the covered work, unless you entered into that arrangement,
or
that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting
any implied license or other defenses to infringement that may
otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or
otherwise) that contradict the conditions of this License, they do not
excuse you from the conditions of this License. If you cannot convey a
covered work so as to satisfy simultaneously your obligations under this
License and any other pertinent obligations, then as a consequence you may
not convey it at all. For example, if you agree to terms that obligate you
to collect a royalty for further conveying from those to whom you convey
the Program, the only way you could satisfy both those terms and this
License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have
permission to link or combine any covered work with a work licensed
under version 3 of the GNU Affero General Public License into a single
combined work, and to convey the resulting work. The terms of this
License will continue to apply to the part which is the covered work,
but the special requirements of the GNU Affero General Public License,
section 13, concerning interaction through a network will apply to the
combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of
the GNU General Public License from time to time. Such new versions will
be similar in spirit to the present version, but may differ in detail to
address new problems or concerns.

Each version is given a distinguishing version number. If the
Program specifies that a certain numbered version of the GNU General
Public License "or any later version" applies to it, you

have the
option of following the terms and conditions either of that numbered
version or of any later version published by the Free Software
Foundation. If the Program does not specify a version number of the
GNU General Public License, you may choose any version ever published
by the Free Software Foundation.

If the Program specifies that a proxy can decide which future
versions of the GNU General Public License can be used, that proxy's
public statement of acceptance of a version permanently authorizes you
to choose that version for the Program.

Later license versions may give you additional or different
permissions. However, no additional obligations are imposed on any
author or copyright holder as a result of your choosing to follow a
later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY
APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT
HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS"
WITHOUT WARRANTY
OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM
IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF
ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING
WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS
THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY
GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE
USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF
DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD
PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS),
EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF
SUCH DAMAGES.

17.
Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided
above cannot be given local legal effect according to their terms,
reviewing courts shall apply local law that most closely approximates
an absolute waiver of all civil liability in connection with the

Program, unless a warranty or assumption of liability accompanies a
copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest
possible use to the public, the best way to achieve this is to make it
free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest
to attach them to the start of each source file to most effectively
state the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where
the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation, either version 3 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program. If not, see <https://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>
This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school,

if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<https://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what you want to
do, use the GNU Lesser General
Public License instead of this License. But first, please read
<https://www.gnu.org/philosophy/why-not-lgpl.html>.

1.78 libnet 1.2

1.78.1 Available under license :

$Id: COPYING,v 1.1.1.1 2003/06/26 21:55:10 route Exp $

libnet 1.1.x
Copyright (c) 1998 - 2002 Mike D. Schiffman <mike@infonexus.com>
http://www.packetfactory.net/libnet
LIBNET 1.1.3+ (c) 2009 - 2012 Sam Roberts <vieuxtech@gmail.com>

All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

EOF

1.79 linux-kernel 4.10.17

1.79.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it. (Some other Free Software Foundation software is covered by
the GNU Library General Public License instead.) You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price. Our General Public Licenses are designed
to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid
anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate to certain responsibilities for you if you
distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether
gratis or for a fee, you must give the recipients all the rights that
you have. You must make sure that they, too, receive or can get the
source code. And you must show them these terms so they know their
rights.

We protect your rights with two steps: (1) copyright the software, and
(2) offer you this license which gives you legal permission to copy,

distribute
and/or modify the software.

Also, for each author's protection and ours, we want to make certain
that everyone understands that there is no warranty for this free
software. If the software is modified by someone else and passed on, we
want its recipients to know that what they have is not the original, so
that any problems introduced by others will not reflect on the original
authors' reputations.

Finally, any free program is threatened constantly by software
patents. We wish to avoid the danger that redistributors of a free
program will individually obtain patent licenses, in effect making the
program proprietary. To prevent this, we have made it clear that any
patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and
modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which
contains
a notice placed by the copyright holder saying it may be distributed
under the terms of this General Public License. The "Program", below,
refers to any such program or work, and a "work based on the Program"
means either the Program or any derivative work under copyright law:
that is to say, a work containing the Program or a portion of it,
either verbatim or with modifications and/or translated into another
language. (Hereinafter, translation is included without limitation in
the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not
covered by this License; they are outside its scope. The act of
running the Program is not restricted, and the output from the Program
is covered only if its contents constitute a work based on the
Program (independent of having been made by running the Program).
Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies
of the Program's
source code as you receive it, in any medium, provided that you
conspicuously and appropriately publish on each copy an appropriate
copyright notice and disclaimer of warranty; keep intact all the
notices that refer to this License and to the absence of any warranty;
and give any other recipients of the Program a copy of this License
along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole
or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered
independent and separate works in
themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under

the scope of this License.

3. You may copy and distribute the Program (or a work based on it,
under Section 2) in object code or executable form under the terms of
Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or
executable form with such
an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the
source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under

this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing

to distribute software through
any other system and a licensee cannot
impose that choice.

This section is intended to make thoroughly clear what is believed to
be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in
certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Program under this License
may add an explicit geographical distribution limitation excluding
those countries, so that distribution is permitted only in or among
countries not thus excluded. In such case, this License incorporates
the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions
of the General Public License from time to time. Such new versions will
be similar in spirit to the present version, but may differ in detail to
address new problems or concerns.

Each version is given a distinguishing version number. If the Program
specifies a version number
of this License which applies to it and "any
later version", you have the option of following the terms and conditions
either of that version or of any later version published by the Free
Software Foundation. If the Program does not specify a version number of
this License, you may choose any version ever published by the Free Software
Foundation.

10. If you wish to incorporate parts of the Program into other free
programs whose distribution conditions are different, write to the author
to ask for permission. For software which is copyrighted by the Free
Software Foundation, write to the Free Software Foundation; we sometimes
make exceptions for this. Our decision will be guided by the two goals
of preserving the free status of all derivatives of our free software and
of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY
FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW.
EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES
PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED
OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS
TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE
PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING,

REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN
IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this

when it starts in an interactive mode:

```
Gnomovision version 69, Copyright (C) year  name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.
```

The hypothetical commands `show w' and
`show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

```
Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice
```

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this is what you want to do, use the GNU Library General
Public License instead of this License.

1.80 fontconfig 2.12.1

1.80.1 Available under license :

fontconfig/COPYING

```
Copyright  2000,2001,2002,2003,2004,2006,2007 Keith Packard
Copyright  2005 Patrick Lam
Copyright  2009 Roozbeh Pournader
Copyright  2008,2009 Red Hat, Inc.
Copyright  2008 Danilo egan
Copyright  2012 Google, Inc.
```

Permission to use, copy, modify, distribute, and sell this software and its
documentation for any purpose is hereby granted without fee, provided that
the above copyright notice appear in all copies and that both that
copyright notice and this permission notice appear in supporting
documentation, and that the name of the author(s) not be used in

advertising or publicity pertaining to distribution of the software without
specific, written prior permission. The authors make no
representations about the suitability of this software for any purpose. It
is provided "as is" without express or implied warranty.

THE AUTHOR(S) DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE,
INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO
EVENT SHALL
 THE AUTHOR(S) BE LIABLE FOR ANY SPECIAL, INDIRECT OR
CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE,
DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER
TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

1.81 linux-kernel 4.8.28

1.81.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it. (Some other Free Software Foundation software is covered by
the GNU Lesser General Public License instead.)
 You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price. Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid
anyone to deny you these rights or to ask you to surrender the rights.

These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program

is covered only if its contents constitute a work based on the
Program (independent of having been made by running the Program).
Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's
source code as you receive it, in any medium, provided that you
conspicuously and appropriately publish on each copy an appropriate
copyright notice and disclaimer of warranty;
keep intact all the
notices that refer to this License and to the absence of any warranty;
and give any other recipients of the Program a copy of this License
along with the Program.

You may charge a fee for the physical act of transferring a copy, and
you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion
of it, thus forming a work based on the Program, and copy and
distribute such modifications or work under the terms of Section 1
above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices
stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in
whole or in part contains or is
derived from the Program or any
part thereof, to be licensed as a whole at no charge to all third
parties under the terms of this License.

c) If the modified program normally reads commands interactively
when run, you must cause it, when started running for such
interactive use in the most ordinary way, to print or display an
announcement including an appropriate copyright notice and a
notice that there is no warranty (or else, saying that you provide
a warranty) and that users may redistribute the program under
these conditions, and telling the user how to view a copy of this
License. (Exception: if the Program itself is interactive but
does not normally print such an announcement, your work based on
the Program is not required to print an announcement.)

These requirements apply to the modified
work as a whole. If
identifiable sections of that work are not derived from the Program,
and can be reasonably considered independent and separate works in
themselves, then this License, and its terms, do not apply to those
sections when you distribute them as separate works. But when you
distribute the same sections as part of a whole which is a work based

on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation
of another work not based on the Program
with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete

machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a

special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License.
However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author

to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals

of preserving the free status of all derivatives of our free software and
of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY
FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES
PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED
OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS
TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH
YOU. SHOULD THE
PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING,
REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING
WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR
REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES,
INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING
OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED
TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY
YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER
PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE
POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest
possible use to the public, the best way to achieve this is to make it
free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest
to attach them to the start of each source file to most effectively
convey the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation; either version 2 of the License, or
(at your option)

any later version.

  This program is distributed in the hope that it will be useful,
  but WITHOUT ANY WARRANTY; without even the implied warranty of
  MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
  GNU General Public License for more details.

  You should have received a copy of the GNU General Public License along
  with this program; if not, write to the Free Software Foundation, Inc.,
  51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

  Gnomovision version 69, Copyright (C) year name of author
  Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.
  This
 is free software, and you are welcome to redistribute it
  under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than 'show w' and 'show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

 Yoyodyne, Inc., hereby disclaims all copyright interest in the program
 'Gnomovision' (which makes passes at compilers) written by James Hacker.
 <signature of Ty Coon>, 1 April 1989
 Ty Coon, President of Vice

This General Public License
 does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this is what you want to do, use the GNU Lesser General
Public License instead of this License.

1.82 jansson 2.7

1.82.1 Available under license :

Copyright (c) 2009-2018 Petri Lehtinen <petri@digip.org>

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR
IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.

1.83 file 5.27

1.83.1 Available under license :

$File: LEGAL.NOTICE,v 1.15 2006/05/03 18:48:33 christos Exp $
Copyright (c) Ian F. Darwin 1986, 1987, 1989, 1990, 1991, 1992, 1994, 1995.
Software written by Ian F. Darwin and others;
maintained 1994- Christos Zoulas.

This software is not subject to any export provision of the United States
Department of Commerce, and may be exported to any country or planet.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
notice immediately at the beginning of the file, without modification,
this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS
OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE

ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

1.84 libpcap 1.7.4

1.84.1 Available under license :

License: BSD

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

1.85 cronie 1.5.1

1.85.1 Available under license :

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

1.86 diffutils 3.4

1.86.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for
software and other kinds of works.

The licenses for most software and other practical works are designed
to take away your freedom to share and change the works. By contrast,
the GNU General Public License is intended to guarantee your freedom to
share and change all versions of a program--to make sure it remains free
software for all its users. We, the Free Software Foundation, use the
GNU General Public License for most of our software; it applies also to
any other work released this way by its authors. You can apply it to
your programs, too.

When we speak of free software, we are referring to
freedom, not
price. Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
them if you wish), that you receive source code or can get it if you
want it, that you can change the software or use pieces of it in new
free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you
these rights or asking you to surrender the rights. Therefore, you have
certain responsibilities if you distribute copies of the software, or if
you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1)
assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand
ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of

packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works

for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a

copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent

the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you

must place, in the relevant source files, a statement of the
additional terms that apply to those files, or a notice indicating
where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the
form of a separately written license, or stated as exceptions;
the above
requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly
provided under this License. Any attempt otherwise to propagate or
modify it is void, and will automatically terminate your rights under
this License (including any patent licenses granted under the third
paragraph of section 11).

However, if you cease all violation of this License, then your
license from a particular copyright holder is reinstated (a)
provisionally, unless and until the copyright holder explicitly and
finally terminates your license, and (b) permanently, if the copyright
holder fails to notify you of the violation by some reasonable means
prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is
reinstated permanently if the copyright holder notifies you of the
violation by some reasonable means, this is the first time you have
received notice of violation of this License (for any work) from that
copyright
holder, and you cure the violation prior to 30 days after
your receipt of the notice.

Termination of your rights under this section does not terminate the
licenses of parties who have received copies or rights from you under
this License. If your rights have been terminated and not permanently
reinstated, you do not qualify to receive new licenses for the same
material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or
run a copy of the Program. Ancillary propagation of a covered work
occurring solely as a consequence of using peer-to-peer transmission
to receive a copy likewise does not require acceptance. However,
nothing other than this License grants you permission to propagate or
modify any covered work. These actions infringe copyright if you do
not accept this License. Therefore, by modifying or propagating a
covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights
granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For
purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and

propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or

that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's

public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY
OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17.
Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it

free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest
to attach them to the start of each source file to most effectively
state the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where
the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation, either version 3 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>
This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what you want to

do, use the GNU Lesser General
Public License instead of this License. But first, please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.
@c The GNU Free Documentation License.
@center Version 1.3, 3 November 2008

@c This file is intended to be included within another document,
@c hence no sectioning command or @node.

@display
Copyright @copyright{} 2000, 2001, 2002, 2007, 2008 Free Software Foundation, Inc.
@uref{http://fsf.org/}

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.
@end display

@enumerate 0
@item
PREAMBLE

The purpose of this License is to make a manual, textbook, or other
functional and useful document @dfn{free} in the sense of freedom: to
assure everyone the effective freedom to copy and redistribute it,
with or without modifying it, either commercially or noncommercially.
Secondarily, this License preserves for the author and publisher a way
to get credit for their work, while not being considered responsible
for modifications made by others.

This License is a kind of ``copyleft'', which means that derivative
works of the document
must themselves be free in the same sense. It
complements the GNU General Public License, which is a copyleft
license designed for free software.

We have designed this License in order to use it for manuals for free
software, because free software needs free documentation: a free
program should come with manuals providing the same freedoms that the
software does. But this License is not limited to software manuals;
it can be used for any textual work, regardless of subject matter or
whether it is published as a printed book. We recommend this License
principally for works whose purpose is instruction or reference.

@item
APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that
contains a notice placed by the copyright holder saying it can be

distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The ``Document'', below, refers
to any such manual or work. Any member of the public is a licensee, and is addressed as ``you''. You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A ``Modified Version'' of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A ``Secondary Section'' is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political
position regarding
them.

The ``Invariant Sections'' are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The ``Cover Texts'' are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A ``Transparent'' copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for
images composed of
pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart

or discourage subsequent modification by readers is not Transparent.
An image format is not Transparent if used for any substantial amount
of text. A copy that is not ``Transparent'' is called ``Opaque''.

Examples of suitable formats for Transparent copies include plain
ASCII without markup, Texinfo input format, La@TeX{} input
format, SGML or XML using a publicly available
DTD, and standard-conforming simple HTML,
PostScript or PDF designed for human modification. Examples
of transparent image formats include PNG, XCF and
JPG@. Opaque formats include proprietary formats that can be
read and edited only by proprietary word
 processors, SGML or
XML for which the DTD and/or processing tools are
not generally available, and the machine-generated HTML,
PostScript or PDF produced by some word processors for
output purposes only.

The ``Title Page'' means, for a printed book, the title page itself,
plus such following pages as are needed to hold, legibly, the material
this License requires to appear in the title page. For works in
formats which do not have any title page as such, ``Title Page'' means
the text near the most prominent appearance of the work's title,
preceding the beginning of the body of the text.

The ``publisher'' means any person or entity that distributes copies
of the Document to the public.

A section ``Entitled XYZ'' means a named subunit of the Document whose
title either is precisely XYZ or contains XYZ in parentheses following
text that translates XYZ in another language. (Here XYZ stands for a
specific section name mentioned below, such as ``Acknowledgements'',
``Dedications'', ``Endorsements'',
 or ``History''.)  To ``Preserve the Title''
of such a section when you modify the Document means that it remains a
section ``Entitled XYZ'' according to this definition.

The Document may include Warranty Disclaimers next to the notice which
states that this License applies to the Document. These Warranty
Disclaimers are considered to be included by reference in this
License, but only as regards disclaiming warranties: any other
implication that these Warranty Disclaimers may have is void and has
no effect on the meaning of this License.

@item
VERBATIM COPYING

You may copy and distribute the Document in any medium, either

commercially or noncommercially, provided that this License, the
copyright notices, and the license notice saying this License applies
to the Document are reproduced in all copies, and that you add no other
conditions whatsoever to those of this License. You may not use
technical measures to obstruct or control the reading or further
copying of the copies
you make or distribute. However, you may accept
compensation in exchange for copies. If you distribute a large enough
number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and
you may publicly display copies.

@item
COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have
printed covers) of the Document, numbering more than 100, and the
Document's license notice requires Cover Texts, you must enclose the
copies in covers that carry, clearly and legibly, all these Cover
Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on
the back cover. Both covers must also clearly and legibly identify
you as the publisher of these copies. The front cover must present
the full title with all words of the title equally prominent and
visible. You may add other material on the covers in addition.
Copying with changes limited to the covers, as long as they preserve
the
title of the Document and satisfy these conditions, can be treated
as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit
legibly, you should put the first ones listed (as many as fit
reasonably) on the actual cover, and continue the rest onto adjacent
pages.

If you publish or distribute Opaque copies of the Document numbering
more than 100, you must either include a machine-readable Transparent
copy along with each Opaque copy, or state in or with each Opaque copy
a computer-network location from which the general network-using
public has access to download using public-standard network protocols
a complete Transparent copy of the Document, free of added material.
If you use the latter option, you must take reasonably prudent steps,
when you begin distribution of Opaque copies in quantity, to ensure
that this Transparent copy will remain thus accessible at the stated
location until at least one year after the last time you distribute
an
Opaque copy (directly or through your agents or retailers) of that
edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

@item
MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

@enumerate A
@item
Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same
title as a previous version
if the original publisher of that version gives permission.

@item
List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

@item
State on the Title page the name of the publisher of the Modified Version, as the publisher.

@item
Preserve all the copyright notices of the Document.

@item
Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

@item
Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

@item

Preserve in that license notice the full lists of Invariant Sections
and required Cover Texts given in the
Document's license notice.

@item
Include an unaltered copy of this License.

@item
Preserve the section Entitled ``History'', Preserve its Title, and add
to it an item stating at least the title, year, new authors, and
publisher of the Modified Version as given on the Title Page. If
there is no section Entitled ``History'' in the Document, create one
stating the title, year, authors, and publisher of the Document as
given on its Title Page, then add an item describing the Modified
Version as stated in the previous sentence.

@item
Preserve the network location, if any, given in the Document for
public access to a Transparent copy of the Document, and likewise
the network locations given in the Document for previous versions
it was based on. These may be placed in the ``History'' section.
You may omit a network location for a work that was published at
least four years before the Document itself, or if the original
publisher of the version it refers to gives permission.

@item
For any
section Entitled ``Acknowledgements'' or ``Dedications'', Preserve
the Title of the section, and preserve in the section all the
substance and tone of each of the contributor acknowledgements and/or
dedications given therein.

@item
Preserve all the Invariant Sections of the Document,
unaltered in their text and in their titles. Section numbers
or the equivalent are not considered part of the section titles.

@item
Delete any section Entitled ``Endorsements''. Such a section
may not be included in the Modified Version.

@item
Do not retitle any existing section to be Entitled ``Endorsements'' or
to conflict in title with any Invariant Section.

@item
Preserve any Warranty Disclaimers.
@end enumerate

If the Modified Version includes new front-matter sections or
appendices that qualify as Secondary Sections and contain no material
copied from the Document, you may at your option designate some or all
of these sections as invariant. To do this, add their titles to the
list of Invariant
 Sections in the Modified Version's license notice.
These titles must be distinct from any other section titles.

You may add a section Entitled ``Endorsements", provided it contains
nothing but endorsements of your Modified Version by various
parties---for example, statements of peer review or that the text has
been approved by an organization as the authoritative definition of a
standard.

You may add a passage of up to five words as a Front-Cover Text, and a
passage of up to 25 words as a Back-Cover Text, to the end of the list
of Cover Texts in the Modified Version. Only one passage of
Front-Cover Text and one of Back-Cover Text may be added by (or
through arrangements made by) any one entity. If the Document already
includes a cover text for the same cover, previously added by you or
by arrangement made by the same entity you are acting on behalf of,
you may not add another; but you may replace the old one, on explicit
permission from the previous publisher that added the old
 one.

The author(s) and publisher(s) of the Document do not by this License
give permission to use their names for publicity for or to assert or
imply endorsement of any Modified Version.

@item
COMBINING DOCUMENTS

You may combine the Document with other documents released under this
License, under the terms defined in section 4 above for modified
versions, provided that you include in the combination all of the
Invariant Sections of all of the original documents, unmodified, and
list them all as Invariant Sections of your combined work in its
license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and
multiple identical Invariant Sections may be replaced with a single
copy. If there are multiple Invariant Sections with the same name but
different contents, make the title of each such section unique by
adding at the end of it, in parentheses, the name of the original
author or publisher of that section if
 known, or else a unique number.
Make the same adjustment to the section titles in the list of

Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled ``History''
in the various original documents, forming one section Entitled
``History''; likewise combine any sections Entitled ``Acknowledgements'',
and any sections Entitled ``Dedications''. You must delete all
sections Entitled ``Endorsements.''

@item
COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents
released under this License, and replace the individual copies of this
License in the various documents with a single copy that is included in
the collection, provided that you follow the rules of this License for
verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute
it individually under this License, provided you insert a copy of this
License
 into the extracted document, and follow this License in all
other respects regarding verbatim copying of that document.

@item
AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate
and independent documents or works, in or on a volume of a storage or
distribution medium, is called an ``aggregate'' if the copyright
resulting from the compilation is not used to limit the legal rights
of the compilation's users beyond what the individual works permit.
When the Document is included in an aggregate, this License does not
apply to the other works in the aggregate which are not themselves
derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these
copies of the Document, then if the Document is less than one half of
the entire aggregate, the Document's Cover Texts may be placed on
covers that bracket the Document within the aggregate, or the
electronic equivalent of covers if the Document is in electronic
 form.
Otherwise they must appear on printed covers that bracket the whole
aggregate.

@item
TRANSLATION

Translation is considered a kind of modification, so you may

distribute translations of the Document under the terms of section 4.
Replacing Invariant Sections with translations requires special
permission from their copyright holders, but you may include
translations of some or all Invariant Sections in addition to the
original versions of these Invariant Sections. You may include a
translation of this License, and all the license notices in the
Document, and any Warranty Disclaimers, provided that you also include
the original English version of this License and the original versions
of those notices and disclaimers. In case of a disagreement between
the translation and the original version of this License or a notice
or disclaimer, the original version will prevail.

If a section in the Document is Entitled ``Acknowledgements",
``Dedications", or ``History", the requirement
 (section 4) to Preserve
its Title (section 1) will typically require changing the actual
title.

@item
TERMINATION

You may not copy, modify, sublicense, or distribute the Document
except as expressly provided under this License. Any attempt
otherwise to copy, modify, sublicense, or distribute it is void, and
will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license
from a particular copyright holder is reinstated (a) provisionally,
unless and until the copyright holder explicitly and finally
terminates your license, and (b) permanently, if the copyright holder
fails to notify you of the violation by some reasonable means prior to
60 days after the cessation.

Moreover, your license from a particular copyright holder is
reinstated permanently if the copyright holder notifies you of the
violation by some reasonable means, this is the first time you have
received notice of violation of this License (for
 any work) from that
copyright holder, and you cure the violation prior to 30 days after
your receipt of the notice.

Termination of your rights under this section does not terminate the
licenses of parties who have received copies or rights from you under
this License. If your rights have been terminated and not permanently
reinstated, receipt of a copy of some or all of the same material does
not give you any rights to use it.

@item

FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions
of the GNU Free Documentation License from time to time. Such new
versions will be similar in spirit to the present version, but may
differ in detail to address new problems or concerns. See
@uref{http://www.gnu.org/copyleft/}.

Each version of the License is given a distinguishing version number.
If the Document specifies that a particular numbered version of this
License ``or any later version'' applies to it, you have the option of
following the terms and
conditions either of that specified version or
of any later version that has been published (not as a draft) by the
Free Software Foundation. If the Document does not specify a version
number of this License, you may choose any version ever published (not
as a draft) by the Free Software Foundation. If the Document
specifies that a proxy can decide which future versions of this
License can be used, that proxy's public statement of acceptance of a
version permanently authorizes you to choose that version for the
Document.

@item
RELICENSING

``Massive Multiauthor Collaboration Site'' (or ``MMC Site'') means any
World Wide Web server that publishes copyrightable works and also
provides prominent facilities for anybody to edit those works. A
public wiki that anybody can edit is an example of such a server. A
``Massive Multiauthor Collaboration'' (or ``MMC'') contained in the
site means any set of copyrightable works thus published on the MMC
site.

``CC-BY-SA'' means the Creative Commons
Attribution-Share Alike 3.0
license published by Creative Commons Corporation, a not-for-profit
corporation with a principal place of business in San Francisco,
California, as well as future copyleft versions of that license
published by that same organization.

``Incorporate'' means to publish or republish a Document, in whole or
in part, as part of another Document.

An MMC is ``eligible for relicensing'' if it is licensed under this
License, and if all works that were first published under this License
somewhere other than this MMC, and subsequently incorporated in whole
or in part into the MMC, (1) had no cover texts or invariant sections,
and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site
under CC-BY-SA on the same site at any time before August 1, 2009,
provided the MMC is eligible for relicensing.

@end enumerate

@page
@heading ADDENDUM: How to use this License for your documents

To use this License
 in a document you have written, include a copy of
the License in the document and put the following copyright and
license notices just after the title page:

@smallexample
@group
 Copyright (C) @var{year} @var{your name}.
 Permission is granted to copy, distribute and/or modify this document
 under the terms of the GNU Free Documentation License, Version 1.3
 or any later version published by the Free Software Foundation;
 with no Invariant Sections, no Front-Cover Texts, and no Back-Cover
 Texts. A copy of the license is included in the section entitled ``GNU
 Free Documentation License".
@end group
@end smallexample

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts,
replace the ``with@dots{}Texts."@: line with this:

@smallexample
@group
   with the Invariant Sections being @var{list their titles}, with
   the Front-Cover Texts being @var{list}, and with the Back-Cover Texts
   being @var{list}.
@end group
@end smallexample

If you have Invariant
 Sections without Cover Texts, or some other
combination of the three, merge those two alternatives to suit the
situation.

If your document contains nontrivial examples of program code, we
recommend releasing these examples in parallel under your choice of
free software license, such as the GNU General Public License,
to permit their use in free software.

@c Local Variables:
@c ispell-local-pdict: "ispell-dict"
@c End:

1.87 libcheck 0.10.0

1.87.1 Available under license :

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts
as the successor of the GNU Library Public License, version 2, hence
the version number 2.1.]

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
Licenses are intended to guarantee your freedom to share and change
free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some
specially designated software packages--typically libraries--of the
Free Software Foundation and other authors who decide
to use it. You
can use it too, but we suggest you first think carefully about whether
this license or the ordinary General Public License is the better
strategy to use in any particular case, based on the explanations
below.

When we speak of free software, we are referring to freedom of use,
not price. Our General Public Licenses are designed to make sure that
you have the freedom to distribute copies of free software (and charge
for this service if you wish); that you receive source code or can get
it if you want it; that you can change the software and use pieces of
it in new free programs; and that you are informed that you can do
these things.

To protect your rights, we need to make restrictions that forbid
distributors to deny you these rights or to ask you to surrender these
rights. These restrictions translate to certain responsibilities for

you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General

Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work

which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another
language. (Hereinafter, translation is
included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium,
provided that
you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms

of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably
considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary
GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object
code for the work under the terms of Section 6.
Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the
work with the complete corresponding
machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly
with a modified version of the library, if
the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally
distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any
other library
facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot

impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU
FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively
convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301

USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or
your school, if any, to sign a "copyright disclaimer" for the library,
if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the
library `Frob' (a library for tweaking knobs) written by James
Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

1. Redistributions of source code must retain the copyright
  notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products
  derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
NOT LIMITED TO, PROCUREMENT
 OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF
THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

1.88 libpciaccess 0.13.4

1.88.1 Available under license :

MIT License

Copyright (c) <year> <copyright holders>

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR
IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.
(C) Copyright IBM Corporation 2006, 2007
(C) Copyright Eric Anholt 2006
(C) Copyright Mark Kettenis 2011
(C) Copyright Robert Millan 2012
Copyright (c) 2007, 2008, 2009, 2011, 2012, 2013 Oracle and/or its affiliates.
Copyright 2009, 2012 Red Hat, Inc.
All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to
deal in the Software without restriction, including without limitation on
the rights to use, copy, modify, merge, publish, distribute, sub license,
and/or sell copies of the Software, and to permit persons to whom the
Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice (including the next
paragraph) shall be included in all copies or substantial portions of the
Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IN NO EVENT SHALL
IBM AND/OR THEIR SUPPLIERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING
FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS
IN THE SOFTWARE.

Copyright (c) 2008 Juan Romero Pardines
Copyright (c) 2008, 2011 Mark Kettenis
Copyright (c) 2009 Michael Lorenz
Copyright (c) 2009, 2012 Samuel Thibault

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES
WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR
ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF
OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (C) 2000 The XFree86 Project, Inc. All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to
deal in the Software without restriction, including without limitation the
rights to use, copy, modify, merge, publish, distribute, sublicense, and/or
sell copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS",
WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
XFREE86 PROJECT BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER
IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN
CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of the XFree86 Project shall
not be used in advertising or otherwise to promote the sale, use or other
dealings in this Software without prior written authorization from the
XFree86 Project.

Copyright (c) 2007 Paulo R. Zanoni, Tiago Vignatti
Copyright (c) 2009 Tiago Vignatti

Permission is hereby granted, free of charge, to any person
obtaining a copy of this software and associated documentation
files (the "Software"), to deal in the Software without
restriction,
including without limitation the rights to use,
copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the
Software is furnished to do so, subject to the following
conditions:

The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES
OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY,
WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING
FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR
OTHER DEALINGS IN THE SOFTWARE.

1.89 bind 9.11.6

1.89.1 Available under license :

Redistribution terms Automated Testing Framework
==========

License
****

Copyright (c) 2007, 2008, 2009, 2010, 2011, 2012 The NetBSD Foundation, Inc.
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice,
this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE NETBSD FOUNDATION, INC. AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
IN NO EVENT SHALL THE FOUNDATION OR CONTRIBUTORS
BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright 2011, 2012 Google Inc.
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation
and/or other materials provided with the distribution.

* Neither the name of Google Inc. nor the names of its contributors
may be used to endorse or promote products derived from this software
without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Relicensed

code
****

The following code snippets have been taken from other projects. Even
though they were not originally licensed under the terms above, the
original authors have agreed to relicense their work so that this project
can be distributed under a single license. This section is put here just to
clarify this fact.

* configure.ac, Makefile.am: The original versions were derived from the
ones in the XML Catalog Manager project, version 2.2.

Author: Julio Merino <jmmv@users.sourceforge.net>

* atf-c/ui.c: The format_paragraph and format_text functions were
derived form the ones in the Monotone project, revision
3a0982da308228d796df35f98d787c5cff2bb5b6.

Author: Julio Merino <jmmv@NetBSD.org>

* atf-c++/detail/io.hpp, atf-c++/detail/io.cpp, atf-c++/detail/io_test.cpp:
These files were derived from the file_handle, systembuf, pipe and pistream
classes and tests found in the Boost.Process library.

Author: Julio Merino <jmmv84@gmail.com>

* admin/check-style.sh,
admin/check-style-common.awk,
admin/check-style-cpp.awk, admin/check-style-shell.awk: These files,
except the first one, were first implemented in the Buildtool project.
They were later adapted to be part of Boost.Process and, during that
process, the shell script was created.

Author: Julio Merino <jmmv84@gmail.com>

==========

vim: filetype=text:textwidth=75:expandtab:shiftwidth=2:softtabstop=2
Mozilla Public License, version 2.0

1. Definitions

1.1. "Contributor"

means each individual or legal entity that creates, contributes to the
creation of, or owns Covered Software.

1.2. "Contributor Version"

means the combination of the Contributions of others (if any) used by a Contributor and that particular Contributor's Contribution.

1.3. "Contribution"

means Covered Software of a particular Contributor.

1.4. "Covered Software"

means Source Code Form to which the initial Contributor has attached the notice in Exhibit A, the Executable Form of such Source Code Form, and Modifications of such Source Code Form, in each case including portions thereof.

1.5. "Incompatible With Secondary Licenses"
means

a. that the initial Contributor has attached the notice described in Exhibit B to the Covered Software; or

b. that the Covered Software was made available under the terms of version 1.1 or earlier of the
License, but not also under the terms of
a Secondary License.

1.6. "Executable Form"

means any form of the work other than Source Code Form.

1.7. "Larger Work"

means a work that combines Covered Software with other material, in a separate file or files, that is not Covered Software.

1.8. "License"

means this document.

1.9. "Licensable"

means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently, any and all of the rights conveyed by this License.

1.10. "Modifications"

means any of the following:

a. any file in Source Code Form that results from an addition to, deletion from, or modification of the contents of Covered Software; or

b. any new file in Source Code Form that contains any Covered Software.

1.11. "Patent Claims" of a Contributor

means any patent claim(s), including without limitation, method, process, and apparatus claims, in any patent Licensable by such Contributor that would be infringed, but for the grant of the License, by the making, using, selling, offering for sale, having made, import, or transfer of either its Contributions or its Contributor Version.

1.12. "Secondary License"

means either the GNU General Public License, Version 2.0, the GNU Lesser General Public License, Version 2.1, the GNU Affero General Public License, Version 3.0, or any later versions of those licenses.

1.13. "Source Code Form"

means the form of the work preferred for making modifications.

1.14. "You" (or "Your")

means an individual or a legal entity exercising rights under this License. For legal entities, "You" includes any entity that controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. License Grants and Conditions

2.1. Grants

Each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license:

a. under intellectual property rights (other than patent or trademark) Licensable by such Contributor to use, reproduce, make available, modify, display, perform, distribute, and otherwise exploit its Contributions, either on an unmodified basis, with Modifications, or

as part of a Larger Work; and

b. under Patent Claims of such Contributor to make, use, sell, offer for sale, have made, import, and otherwise transfer either its Contributions or its Contributor Version.

2.2. Effective Date

The licenses granted in Section 2.1 with respect to any Contribution become effective for each Contribution on the date the Contributor first distributes such Contribution.

2.3. Limitations on Grant Scope

The licenses granted in this Section 2 are the only rights granted under this License. No additional rights or licenses will be implied from the distribution or licensing of Covered Software under this License. Notwithstanding Section 2.1(b) above, no patent license is granted by a Contributor:

a. for any code that a Contributor has removed from Covered Software; or

b. for infringements caused by: (i) Your and any other third party's modifications of Covered Software, or (ii) the combination of its Contributions with other software (except as part of its Contributor Version); or

c. under Patent Claims infringed by Covered Software in the absence of its Contributions.

This License does not grant any rights in the trademarks, service marks, or logos of any Contributor (except as may be necessary to comply with the notice requirements in Section 3.4).

2.4. Subsequent Licenses

No Contributor makes additional grants as a result of Your choice to distribute the Covered Software under a subsequent version of this License (see Section 10.2) or under the terms of a Secondary License (if permitted under the terms of Section 3.3).

2.5. Representation

Each Contributor represents that the Contributor believes its Contributions are its original creation(s) or it has sufficient rights to grant the rights to its Contributions conveyed by this License.

2.6. Fair Use

This License is not intended to limit any rights You have under applicable copyright doctrines of fair use, fair dealing, or other equivalents.

2.7. Conditions

Sections 3.1, 3.2, 3.3, and 3.4 are conditions of the licenses granted in Section 2.1.

3. Responsibilities

3.1. Distribution of Source Form

All distribution of Covered Software in Source Code Form, including any Modifications that You create or to which You contribute, must be under the terms of this License. You must inform recipients that the Source Code Form of the Covered Software is governed by the terms of this License, and how they can obtain a copy of this License. You may not attempt to alter or restrict the recipients' rights in the Source Code Form.

3.2. Distribution of Executable Form

If You distribute Covered Software in Executable Form then:

a. such Covered Software must also be made available in Source Code Form, as described in Section 3.1, and You must inform recipients of the Executable Form how they can obtain a copy of such Source Code Form by reasonable means in a timely manner, at a charge no more than the cost of distribution to the recipient; and

b. You may distribute such Executable Form under the terms of this License, or sublicense it under different terms, provided that the license for the Executable Form does not attempt to limit or alter the recipients' rights in the Source Code Form under this License.

3.3. Distribution of a Larger Work

You may create and distribute a Larger Work under terms of Your choice, provided that You also comply with the requirements of this License for the Covered Software. If the Larger Work is a combination of Covered Software with a work governed by one or more Secondary Licenses, and the

Covered Software is not Incompatible With Secondary Licenses, this License permits You to additionally distribute such Covered Software under the terms of such Secondary License(s), so that the recipient of the Larger Work may, at their option, further distribute the Covered Software under the terms of either this License or such Secondary License(s).

3.4. Notices

You may not remove or alter the substance of any license notices (including copyright notices, patent notices, disclaimers of warranty, or limitations of liability) contained within the Source Code Form of the Covered Software, except that You may alter any license notices to the extent required to remedy known factual inaccuracies.

3.5. Application of Additional Terms

You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Software. However, You may do so only on Your own behalf, and not on behalf of any Contributor. You must make it absolutely clear that any such warranty, support, indemnity, or liability obligation is offered by You alone, and You hereby agree to indemnify every Contributor for any liability incurred by such Contributor as a result of warranty, support, indemnity or liability terms You offer. You may include additional disclaimers of warranty and limitations of liability specific to any jurisdiction.

4. Inability to Comply Due to Statute or Regulation

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Software due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be placed in a text file included with all distributions of the Covered Software under this License. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Termination

5.1. The rights granted under this License will terminate automatically if You fail to comply with any of its terms. However, if You become compliant, then the rights granted under this License from a particular Contributor are reinstated (a) provisionally, unless and until such Contributor

explicitly
and finally terminates Your grants, and (b) on an ongoing basis, if such Contributor fails to notify You of the non-compliance by some reasonable means prior to 60 days after You have come back into compliance. Moreover, Your grants from a particular Contributor are reinstated on an ongoing basis if such Contributor notifies You of the non-compliance by some reasonable means, this is the first time You have received notice of non-compliance with this License from such Contributor, and You become compliant prior to 30 days after Your receipt of the notice.

5.2. If You initiate litigation against any entity by asserting a patent infringement claim (excluding declaratory judgment actions, counter-claims, and cross-claims) alleging that a Contributor Version directly or indirectly infringes any patent, then the rights granted to You by any and all Contributors for the Covered Software under Section 2.1 of this License
shall terminate.

5.3. In the event of termination under Sections 5.1 or 5.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or Your distributors under this License prior to termination shall survive termination.

6. Disclaimer of Warranty

Covered Software is provided under this License on an "as is" basis, without warranty of any kind, either expressed, implied, or statutory, including, without limitation, warranties that the Covered Software is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the Covered Software is with You. Should any Covered Software prove defective in any respect, You (not any Contributor) assume the cost of any necessary servicing, repair, or correction. This disclaimer of warranty constitutes an essential part of this License. No use of any Covered Software is authorized
under
this License except under this disclaimer.

7. Limitation of Liability

Under no circumstances and under no legal theory, whether tort (including negligence), contract, or otherwise, shall any Contributor, or anyone who distributes Covered Software as permitted above, be liable to You for any direct, indirect, special, incidental, or consequential damages of any character including, without limitation, damages for lost profits, loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses, even if such party shall have been informed of the possibility of such damages. This limitation of liability

shall not apply to liability for death or personal injury resulting from such party's negligence to the extent applicable law prohibits such limitation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this exclusion and limitation may not
apply to You.

8. Litigation

Any litigation relating to this License may be brought only in the courts of a jurisdiction where the defendant maintains its principal place of business and such litigation shall be governed by laws of that jurisdiction, without reference to its conflict-of-law provisions. Nothing in this Section shall prevent a party's ability to bring cross-claims or counter-claims.

9. Miscellaneous

This License represents the complete agreement concerning the subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not be used to construe this License against a Contributor.

10. Versions of the License

10.1. New Versions

Mozilla Foundation is the license steward. Except as provided in Section

10.3, no one other than the license steward has the right to modify or publish new versions of this License. Each version will be given a distinguishing version number.

10.2. Effect of New Versions

You may distribute the Covered Software under the terms of the version of the License under which You originally received the Covered Software, or under the terms of any subsequent version published by the license steward.

10.3. Modified Versions

If you create software not governed by this License, and you want to create a new license for such software, you may create and use a modified version of this License if you rename the license and remove

any references to the name of the license steward (except to note that such modified license differs from this License).

10.4. Distributing Source Code Form that is Incompatible With Secondary Licenses If You choose to distribute Source Code Form that is Incompatible
With Secondary Licenses under the terms of this version of the License, the notice described in Exhibit B of this License must be attached.

Exhibit A - Source Code Form License Notice

This Source Code Form is subject to the terms of the Mozilla Public License, v. 2.0. If a copy of the MPL was not distributed with this file, You can obtain one at http://mozilla.org/MPL/2.0/.

If it is not possible or desirable to put the notice in a particular file, then You may include the notice in a location (such as a LICENSE file in a relevant directory) where a recipient would be likely to look for such a notice.

You may add additional accurate notices of copyright ownership.

Exhibit B - "Incompatible With Secondary Licenses" Notice

This Source Code Form is "Incompatible With Secondary Licenses", as defined by the Mozilla Public License, v. 2.0.

```
<!--
- Copyright (C) 2005, 2007, 2009, 2015, 2016  Internet Systems Consortium, Inc. ("ISC")
-
- This Source Code Form is subject to the terms of the Mozilla Public
- License, v. 2.0. If a copy of the MPL was not distributed with this
- file, You can obtain one at http://mozilla.org/MPL/2.0/.
-->

<!-- $Id$ -->

<!-- Generate ISC copyright comments from Docbook copyright metadata. -->

<xsl:stylesheet version="1.0"
 xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
 xmlns:xi="http://www.w3.org/2001/XInclude"
 xmlns:db="http://docbook.org/ns/docbook">
```

```
 <xsl:template name="isc.copyright.format">
   <xsl:param name="text"/>
   <xsl:value-of select="$isc.copyright.leader"/>
   <xsl:value-of select="normalize-space(substring-before($text, '&#10;'))"/>
   <xsl:text>&#10;</xsl:text>
   <xsl:variable name="rest" select="substring-after($text, '&#10;')"/>
   <xsl:if test="translate($rest, '&#9;&#32;', '')">
     <xsl:call-template name="isc.copyright.format">
       <xsl:with-param
 name="text" select="$rest"/>
     </xsl:call-template>
   </xsl:if>
 </xsl:template>

 <xsl:variable name="isc.copyright.text">
   <xsl:text>
      This Source Code Form is subject to the terms of the Mozilla Public
      License, v. 2.0. If a copy of the MPL was not distributed with this
      file, You can obtain one at http://mozilla.org/MPL/2.0/.
   </xsl:text>
 </xsl:variable>

 <xsl:variable name="isc.copyright">
   <xsl:call-template name="isc.copyright.format">
     <xsl:with-param name="text">
       <xsl:for-each select="book/info/copyright | refentry/docinfo/copyright">
   <xsl:text>Copyright (C) </xsl:text>
   <xsl:call-template name="copyright.years">
     <xsl:with-param name="years" select="year"/>
   </xsl:call-template>
   <xsl:text> </xsl:text>
   <xsl:value-of select="holder"/>
        <xsl:value-of select="$isc.copyright.breakline"/>
   <xsl:text>&#10;</xsl:text>
 </xsl:for-each>
 <xsl:value-of select="$isc.copyright.text"/>
     </xsl:with-param>
    </xsl:call-template>
 </xsl:variable>
</xsl:stylesheet>

<!--
 - Local variables:
 - mode: sgml
 - End:
-->
Copyright (C) 1996-2017  Internet Systems Consortium, Inc. ("ISC")
```

This Source Code Form is subject to the terms of the Mozilla Public
License, v. 2.0. If a copy of the MPL was not distributed with this
file, You can obtain one at http://mozilla.org/MPL/2.0/.

Portions of this code release fall under one or more of the
following Copyright notices. Please see individual source
files for details.

For binary releases also see: OpenSSL-LICENSE.

Copyright (C) 1996-2001 Nominum, Inc.

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND NOMINUM DISCLAIMS ALL WARRANTIES
WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL NOMINUM BE LIABLE FOR
ANY SPECIAL, DIRECT,
 INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT
OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (C) 1995-2000 by Network Associates, Inc.

Permission to use, copy, modify, and/or distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC AND NETWORK ASSOCIATES DISCLAIMS
ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE
FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
ACTION OF CONTRACT, NEGLIGENCE OR
 OTHER TORTIOUS ACTION, ARISING OUT OF OR
IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (C) 2002 Stichting NLnet, Netherlands, stichting@nlnet.nl.

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the
above copyright notice and this permission notice appear in all
copies.

THE SOFTWARE IS PROVIDED "AS IS" AND STICHTING NLNET
DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL
STICHTING NLNET BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR
CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS
OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE
USE OR PERFORMANCE OF THIS SOFTWARE.

The development of Dynamically Loadable Zones
(DLZ) for Bind 9 was
conceived and contributed by Rob Butler.

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the
above copyright notice and this permission notice appear in all
copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ROB BUTLER
DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL
ROB BUTLER BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR
CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS
OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE
USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (c) 1987, 1990, 1993, 1994
The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms,
with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors
may be used to endorse or promote products derived from this software

without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES
(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

Copyright (C) The Internet Society 2005. This version of
this module is part of RFC 4178; see the RFC itself for
full legal notices.

(The above copyright notice is per RFC 3978 5.6 (a), q.v.)

Copyright (c) 2004 Masarykova universita
(Masaryk University, Brno, Czech Republic)
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

1. Redistributions of source
code must retain the above copyright notice,
this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

3. Neither the name of the University nor the names of its contributors may
be used to endorse or promote products derived from this software
without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE

LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR
PROFITS; OR BUSINESS
INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1997 - 2003 Kungliga Tekniska Hgskolan
(Royal Institute of Technology, Stockholm, Sweden).
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

3. Neither the name of the
Institute nor the names of its contributors
may be used to endorse or promote products derived from this software
without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE INSTITUTE AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE INSTITUTE OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright
(c) 1998 Doug Rabson
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
  notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF
 USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

Copyright ((c)) 2002, Rice University
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are
met:

  * Redistributions of source code must retain the above copyright
  notice, this list of conditions and the following disclaimer.

  * Redistributions in binary form must reproduce the above
  copyright notice, this list of conditions and the following
  disclaimer in the documentation and/or other materials provided
  with the distribution.

  * Neither the name of Rice University (RICE) nor the names of its

 contributors may be used to endorse or promote products derived
  from this software without specific prior written permission.

This software is provided by RICE and the contributors on an "as is"
basis, without any representations or warranties of any kind, express

or implied including, but not limited to, representations or
warranties of non-infringement, merchantability or fitness for a
particular purpose. In no event shall RICE or contributors be liable
for any direct, indirect, incidental, special, exemplary, or
consequential damages (including, but not limited to, procurement of
substitute goods or services; loss of use, data, or profits; or
business interruption) however caused and on any theory of liability,
whether in contract, strict liability, or tort (including negligence
or otherwise) arising in any way out of the use of this software, even
if advised of the possibility of such damage.

Copyright
(c) 1993 by Digital Equipment Corporation.

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies, and that
the name of Digital Equipment Corporation not be used in advertising or
publicity pertaining to distribution of the document or software without
specific, written prior permission.

THE SOFTWARE IS PROVIDED "AS IS" AND DIGITAL EQUIPMENT CORP. DISCLAIMS ALL
WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES
OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL DIGITAL EQUIPMENT
CORPORATION BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL
DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR
PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS
ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS
SOFTWARE.

Copyright
2000 Aaron D. Gifford. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.
3. Neither the name of the copyright holder nor the names of contributors
may be used to endorse or promote products derived from this software
without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR(S) AND CONTRIBUTOR(S) ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR(S) OR CONTRIBUTOR(S) BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

Copyright (c) 1998 Doug Rabson.
Copyright (c) 2001 Jake Burkholder.
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions
in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

Copyright
(C) 1995, 1996, 1997, and 1998 WIDE Project.
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
  notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.
3. Neither the name of the project nor the names of its contributors
  may be used to endorse or promote products derived from this software
  without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN
 NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

Copyright (c) 1999-2000 by Nortel Networks Corporation

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND NORTEL NETWORKS DISCLAIMS
ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES
OF MERCHANTABILITY
 AND FITNESS. IN NO EVENT SHALL NORTEL NETWORKS
BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES
OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS,
WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION,
ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS
SOFTWARE.

Copyright (c) 2000-2002 Japan Network Information Center. All rights reserved.

By using this file, you agree to the terms and conditions set forth bellow.

LICENSE TERMS AND CONDITIONS

The following License Terms and Conditions apply, unless a different
license is obtained from Japan Network Information Center ("JPNIC"),
a Japanese association, Kokusai-Kougyou-Kanda Bldg 6F, 2-3-4 Uchi-Kanda,
Chiyoda-ku, Tokyo 101-0047, Japan.

1. Use, Modification and Redistribution (including distribution of any
modified or derived work) in source and/or
binary forms is permitted
under this License Terms and Conditions.

2. Redistribution of source code must retain the copyright notices as they
appear in each source code file, this License Terms and Conditions.

3. Redistribution in binary form must reproduce the Copyright Notice,
this License Terms and Conditions, in the documentation and/or other
materials provided with the distribution. For the purposes of binary
distribution the "Copyright Notice" refers to the following language:
"Copyright (c) 2000-2002 Japan Network Information Center. All rights
reserved."

4. The name of JPNIC may not be used to endorse or promote products
derived from this Software without specific prior written approval of
JPNIC.

5. Disclaimer/Limitation of Liability: THIS SOFTWARE IS PROVIDED BY JPNIC
"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE ARE DISCLAIMED.
IN NO EVENT SHALL JPNIC BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Copyright (C) 2004 Nominet, Ltd.

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND NOMINET DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS.
IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Portions Copyright RSA Security Inc.

License to copy and use this software is granted provided that it is identified as "RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki)" in all material mentioning or referencing this software.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki)" in all material mentioning or referencing the derived work.

RSA Security Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

Copyright (c) 1996, David Mazieres <dm@uun.org>
Copyright (c) 2008, Damien Miller <djm@openbsd.org>

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright

(c) 2000-2001 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

1. Redistributions of source code must retain the above copyright
  notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in
  the documentation and/or other materials provided with the
  distribution.

3. All advertising materials mentioning features or use of this
  software must display the following acknowledgment:
  "This product includes software developed by the OpenSSL Project
  for use in the OpenSSL Toolkit. (http://www.OpenSSL.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
  endorse or promote products derived
 from this software without
  prior written permission. For written permission, please contact
  licensing@OpenSSL.org.

5. Products derived from this software may not be called "OpenSSL"
  nor may "OpenSSL" appear in their names without prior written
  permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following
  acknowledgment:
  "This product includes software developed by the OpenSSL Project
  for use in the OpenSSL Toolkit (http://www.OpenSSL.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS" AND ANY
EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
LOSS OF USE, DATA, OR PROFITS;
 OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1995, 1997, 1998 The NetBSD Foundation, Inc.
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
  notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE NETBSD FOUNDATION, INC. AND CONTRIBUTORS
``AS IS" AND ANY
 EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE FOUNDATION OR CONTRIBUTORS
BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

Copyright (C) 2008-2011 Red Hat, Inc.

Permission to use, copy, modify, and/or distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE
 SOFTWARE IS PROVIDED "AS IS" AND Red Hat DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS. IN NO EVENT SHALL Red Hat BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Copyright (c) 2013-2014, Farsight Security, Inc.
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions
and the following disclaimer in the
documentation and/or other materials provided with the distribution.

3. Neither the name of the copyright holder nor the names of its
contributors may be used to endorse or promote products derived from
this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE,
EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 2014 by Farsight Security, Inc.

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
Copyright (C) 1999-2014 Internet Systems Consortium, Inc. ("ISC")

This Source Code Form is subject to the terms of the Mozilla Public

License, v. 2.0. If a copy of the MPL was not distributed with this
file, You can obtain one at http://mozilla.org/MPL/2.0/.

Copyright (C) 2009-2015 Red Hat

Permission to use, copy, modify, and/or distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND AUTHORS DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
Copyright (c) 2005 - 2008, Holger Zuleger HZnet. All rights reserved.

This software is open source.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

Redistributions of source code must retain the above copyright notice,
this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice,
this list of conditions and the following disclaimer in the documentation
and/or other materials provided with the distribution.

Neither the name of Holger Zuleger HZnet nor the names of its contributors may
be used to endorse or promote products derived from this software without
specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED.
 IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE
LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 2000-2002 Japan Network Information Center. All rights reserved.

By using this file, you agree to the terms and conditions set forth bellow.

LICENSE TERMS AND CONDITIONS

The following License Terms and Conditions apply, unless a different
license is obtained from Japan Network Information Center ("JPNIC"),
a Japanese association, Kokusai-Kougyou-Kanda Bldg 6F, 2-3-4 Uchi-Kanda,
Chiyoda-ku, Tokyo 101-0047, Japan.

1. Use, Modification and Redistribution (including distribution of any
modified or derived work) in source and/or binary forms is permitted
under this License Terms and Conditions.

2. Redistribution of source code must retain the copyright notices as they
appear in each source code file, this License Terms and Conditions.

3. Redistribution in binary form must reproduce the Copyright Notice,
this License Terms and Conditions, in the documentation and/or other
materials provided with the distribution. For the purposes of binary
distribution
the "Copyright Notice" refers to the following language:
"Copyright (c) 2000-2002 Japan Network Information Center. All rights reserved."

4. The name of JPNIC may not be used to endorse or promote products
derived from this Software without specific prior written approval of
JPNIC.

5. Disclaimer/Limitation of Liability: THIS SOFTWARE IS PROVIDED BY JPNIC
"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL JPNIC BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE,
EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

1.90 cryptsetup 1.7.2

1.90.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price.
Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which
gives you legal permission to copy,
distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we

want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1

above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices
stating that you changed the files and the date of any change.

b) You must cause
any work that you distribute or publish, that in
whole or in part contains or is derived from the Program or any
part thereof, to be licensed as a whole at no charge to all third
parties under the terms of this License.

c) If the modified program normally reads commands interactively
when run, you must cause it, when started running for such
interactive use in the most ordinary way, to print or display an
announcement including an appropriate copyright notice and a
notice that there is no warranty (or else, saying that you provide
a warranty) and that users may redistribute the program under
these conditions, and telling the user how to view a copy of this
License. (Exception: if the Program itself is interactive but
does not normally print such an announcement, your work based on
the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If
identifiable sections of that work
are not derived from the Program,
and can be reasonably considered independent and separate works in
themselves, then this License, and its terms, do not apply to those
sections when you distribute them as separate works. But when you
distribute the same sections as part of a whole which is a work based
on the Program, the distribution of the whole must be on the terms of
this License, whose permissions for other licensees extend to the
entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest
your rights to work written entirely by you; rather, the intent is to
exercise the right to control the distribution of derivative or
collective works based on the Program.

In addition, mere aggregation of another work not based on the Program
with the Program (or with a work based on the Program) on a volume of
a storage or distribution medium does not bring the other work under
the scope of this License.

3. You may copy and distribute the Program (or a work based on it,
under Section 2) in object code or executable form under the terms of
Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable

source code, which must be distributed under the terms of Sections
1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three
years, to give any third party, for a charge no more than your
cost of physically performing source distribution, a complete
machine-readable copy of the corresponding source code, to be
distributed under the terms of Sections 1 and 2 above on a medium
customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer
to distribute corresponding source code. (This alternative is
allowed only for noncommercial distribution
and only if you
received the program in object code or executable form with such
an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for
making modifications to it. For an executable work, complete source
code means all the source code for all modules it contains, plus any
associated interface definition files, plus the scripts used to
control compilation and installation of the executable. However, as a
special exception, the source code distributed need not include
anything that is normally distributed (in either source or binary
form) with the major components (compiler, kernel, and so on) of the
operating system on which the executable runs, unless that component
itself accompanies the executable.

If distribution of executable or object code is made by offering
access to copy from a designated place, then offering equivalent
access to copy the source code from the same place counts as
distribution of the source
code, even though third parties are not
compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program
except as expressly provided under this License. Any attempt
otherwise to copy, modify, sublicense or distribute the Program is
void, and will automatically terminate your rights under this License.
However, parties who have received copies, or rights, from you under
this License will not have their licenses terminated so long as such
parties remain in full compliance.

5. You are not required to accept this License, since you have not
signed it. However, nothing else grants you permission to modify or
distribute the Program or its derivative works. These actions are
prohibited by law if you do not accept this License. Therefore, by
modifying or distributing the Program (or any work based on the

Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in

certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY

YOU OR
THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU
General Public License as published by
the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute
it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate

parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

 Yoyodyne, Inc., hereby disclaims all copyright interest in the program
 `Gnomovision' (which makes passes at compilers) written by James Hacker.

 <signature of Ty Coon>, 1 April 1989
 Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this
 is what you want to do, use the GNU Lesser General
Public License instead of this License.

In addition, as a special exception, the copyright holders give
permission to link the code of portions of this program with the
OpenSSL library under certain conditions as described in each
individual source file, and distribute linked combinations
including the two.

You must obey the GNU General Public License in all respects
for all of the code used other than OpenSSL. If you modify
file(s) with this exception, you may extend this exception to your
version of the file(s), but you are not obligated to do so. If you
do not wish to do so, delete this exception statement from your
version. If you delete this exception statement from all source
files in the program, then also delete it here.
                GNU LESSER GENERAL PUBLIC LICENSE
                   Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts
as the successor of the GNU Library Public License, version 2, hence
the version number 2.1.]

                        Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software

patents pose a constant threat to the existence of
any free program. We wish to make sure that a company cannot
effectively restrict the users of a free program by obtaining a
restrictive license from a patent holder. Therefore, we insist that
any patent license obtained for a version of the library must be
consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the
ordinary GNU General Public License. This license, the GNU Lesser
General Public License, applies to certain designated libraries, and
is quite different from the ordinary General Public License. We use
this license for certain libraries in order to permit linking those
libraries into non-free programs.

When a program is linked with a library, whether statically or using
a shared library, the combination of the two is legally speaking a
combined work, a derivative of the original library. The ordinary
General Public License therefore permits
such linking only if the
entire combination fits its criteria of freedom. The Lesser General
Public License permits more lax criteria for linking other code with
the library.

We call this license the "Lesser" General Public License because it
does Less to protect the user's freedom than the ordinary General
Public License. It also provides other free software developers Less
of an advantage over competing non-free programs. These disadvantages
are the reason we use the ordinary General Public License for many
libraries. However, the Lesser license provides advantages in certain
special circumstances.

For example, on rare occasions, there may be a special need to
encourage the widest possible use of a certain library, so that it becomes
a de-facto standard. To achieve this, non-free programs must be
allowed to use the library. A more frequent case is that a free
library does the same job as widely used non-free libraries. In this
case, there is little to gain by limiting
the free library to free
software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free
programs enables a greater number of people to use a large body of
free software. For example, permission to use the GNU C Library in
non-free programs enables many more people to use the whole GNU
operating system, as well as its variant, the GNU/Linux operating
system.

Although the Lesser General Public License is Less protective of the

users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's

complete source code as you receive it, in any medium,
provided that
you conspicuously and appropriately publish on each copy an
appropriate copyright notice and disclaimer of warranty; keep intact
all the notices that refer to this License and to the absence of any
warranty; and distribute a copy of this License along with the
Library.

You may charge a fee for the physical act of transferring a copy,
and you may at your option offer warranty protection in exchange for a
fee.

2. You may modify your copy or copies of the Library or any portion
of it, thus forming a work based on the Library, and copy and
distribute such modifications or work under the terms of Section 1
above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices
stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no
charge to all third parties under the
terms of this License.

d) If a facility in the modified Library refers to a function or a
table of data to be supplied by an application program that uses
the facility, other than as an argument passed when the facility
is invoked, then you must make a good faith effort to ensure that,
in the event an application does not supply such function or
table, the facility still operates, and performs whatever part of
its purpose remains meaningful.

(For example, a function in a library to compute square roots has
a purpose that is entirely well-defined independent of the
application. Therefore, Subsection 2d requires that any
application-supplied function or table used by this function must
be optional: if the application does not supply it, the square
root function must still compute square roots.)

These requirements apply to the modified work as a whole. If
identifiable sections of that work are not derived from the Library,
and can be
reasonably considered independent and separate works in
themselves, then this License, and its terms, do not apply to those
sections when you distribute them as separate works. But when you
distribute the same sections as part of a whole which is a work based

on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or

linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany

the work with the complete corresponding
machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate
properly with a modified version of the library, if
the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally
distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not

excuse
you from the conditions of this License. If you cannot
distribute so as to satisfy simultaneously your obligations under this
License and any other pertinent obligations, then as a consequence you
may not distribute the Library at all. For example, if a patent
license would not permit royalty-free redistribution of the Library by
all those who receive copies directly or indirectly through you, then
the only way you could satisfy both it and this License would be to
refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any
particular circumstance, the balance of the section is intended to apply,
and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any
patents or other property right claims or to contest validity of any
such claims; this section has the sole purpose of protecting the
integrity of the free software distribution system
which is
implemented by public license practices. Many people have made
generous contributions to the wide range of software distributed
through that system in reliance on consistent application of that
system; it is up to the author/donor to decide if he or she is willing
to distribute software through any other system and a licensee cannot
impose that choice.

This section is intended to make thoroughly clear what is believed to
be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in
certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Library under this License may add
an explicit geographical distribution limitation excluding those countries,
so that distribution is permitted only in or among countries not thus
excluded. In such case, this License incorporates the limitation as if
written in the body of this License.

13. The Free Software Foundation may publish
revised and/or new
versions of the Lesser General Public License from time to time.
Such new versions will be similar in spirit to the present version,
but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library
specifies a version number of this License which applies to it and
"any later version", you have the option of following the terms and
conditions either of that version or of any later version published by
the Free Software Foundation. If the Library does not specify a

license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision
will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE,
BE LIABLE TO YOU
FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is

safest to attach them to the start of each source file to most effectively
convey
the exclusion of warranty; and each file should have at least the
"copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or
modify it under the terms of the GNU Lesser General Public
License as published by the Free Software Foundation; either
version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public
License along with this library; if not, write to the Free Software
Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301
USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the library, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the
library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

In addition, as a special exception, the copyright holders give
permission to link the code of portions of this program with the
OpenSSL library under certain conditions as described in each
individual source file, and distribute linked combinations
including the two.

You must obey the GNU Lesser General Public License in all respects
for all of the code used other than OpenSSL. If you modify
file(s) with this exception, you may extend this exception to your
version

of the file(s), but you are not obligated to do so. If you
do not wish to do so, delete this exception statement from your
version. If you delete this exception statement from all source
files in the program, then also delete it here.

1.91 libnftnl 1.0.6

1.91.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it. (Some other Free Software Foundation software is covered by
the GNU Library General Public License instead.) You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price. Our General Public Licenses
are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid
anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate to certain responsibilities for you if you
distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether
gratis or for a fee, you must give the recipients all the rights that
you have. You must make sure that they, too, receive or can get the
source code. And you must show them these terms so they know their
rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty;

and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program

with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is

void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on
it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit
royalty-free redistribution of the Program by
all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed

through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software
through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a
version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE
LAW. EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS

TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS),
EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) 19yy <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

```
Gnomovision version 69, Copyright (C) 19yy name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.
```

The hypothetical commands
`show w' and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this is what you want to do, use the GNU Library General
Public License instead of this License.

1.92 procps 3.3.12

1.92.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public

License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price.
Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which
gives you legal permission to copy,
distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such

interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work
are not derived from the Program,
and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution

and only if you
received the program in object code or executable form with such
an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source
code, even though third parties are not
compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing
or modifying
the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing

version number. If the Program
specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE,
THERE IS NO WARRANTY
FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR
THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest
to attach them to the start of each source file to most effectively
convey the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU
General Public License as published by
the Free Software Foundation; either version 2 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License along
with this program; if not, write to the Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute
it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this
is what you want to do, use the GNU Lesser General
Public License instead of this License.

GNU LIBRARY GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the library GPL. It is
numbered 2 because it goes with version 2 of the ordinary GPL.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some specially designated Free Software Foundation software, and to any other libraries whose authors decide to use it. You can use it for your libraries, too.

When
we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library, or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link a program with the library, you must provide complete object files to the recipients so that they

can relink them
with the library, after making changes to the library and recompiling
it. And you must show them these terms so they know their rights.

Our method of protecting your rights has two steps: (1) copyright
the library, and (2) offer you this license which gives you legal
permission to copy, distribute and/or modify the library.

Also, for each distributor's protection, we want to make certain
that everyone understands that there is no warranty for this free
library. If the library is modified by someone else and passed on, we
want its recipients to know that what they have is not the original
version, so that any problems introduced by others will not reflect on
the original authors' reputations.

Finally, any free program is threatened constantly by software
patents. We wish to avoid the danger that companies distributing free
software will individually obtain patent licenses, thus in effect
transforming the program into proprietary software. To prevent this,
we
have made it clear that any patent must be licensed for everyone's
free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary
GNU General Public License, which was designed for utility programs. This
license, the GNU Library General Public License, applies to certain
designated libraries. This license is quite different from the ordinary
one; be sure to read it in full, and don't assume that anything in it is
the same as in the ordinary license.

The reason we have a separate public license for some libraries is that
they blur the distinction we usually make between modifying or adding to a
program and simply using it. Linking a program with a library, without
changing the library, is in some sense simply using the library, and is
analogous to running a utility program or application program. However, in
a textual and legal sense, the linked executable is a combined work, a
derivative of the original library, and the ordinary
General Public License
treats it as such.

Because of this blurred distinction, using the ordinary General
Public License for libraries did not effectively promote software
sharing, because most developers did not use the libraries. We
concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the
users of those programs of all benefit from the free status of the
libraries themselves. This Library General Public License is intended to

permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification
follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

GNU LIBRARY GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below,
refers to any such software library or work
which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from

such a program is covered only if
its contents constitute a work based
on the Library (independent of the use of the Library in a tool for
writing it). Whether that is true depends on what the Library does
and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's
complete source code as you receive it, in any medium, provided that
you conspicuously and appropriately publish on each copy an
appropriate copyright notice and disclaimer of warranty; keep intact
all the notices that refer to this License and to the absence of any
warranty; and distribute a copy of this License along with the
Library.

You may charge a fee for the physical act of transferring a copy,
and you may at your option offer warranty protection in exchange for a
fee.

2. You may modify your copy or copies of the Library or any portion
of it, thus forming a work based on the Library, and copy and
distribute such modifications or work under the terms of Section 1
above, provided that you also
meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices
stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no
charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a
table of data to be supplied by an application program that uses
the facility, other than as an argument passed when the facility
is invoked, then you must make a good faith effort to ensure that,
in the event an application does not supply such function or
table, the facility still operates, and performs whatever part of
its purpose remains meaningful.

(For example, a function in a library to compute square roots has
a purpose that is entirely well-defined independent of the
application. Therefore, Subsection 2d requires that
any
application-supplied function or table used by this function must
be optional: if the application does not supply it, the square
root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of
derivative or
collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the

source code from the same place satisfies the requirement to
distribute the source code, even though third parties are not
compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the
Library, but is designed to work with the Library by being compiled or
linked with it, is called a "work that uses
the Library". Such a
work, in isolation, is not a derivative work of the Library, and
therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library
creates an executable that is a derivative of the Library (because it
contains portions of the Library), rather than a "work that uses the
library". The executable is therefore covered by this License.
Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file
that is part of the Library, the object code for the work may be a
derivative work of the Library even though the source code is not.
Whether this is true is especially significant if the work can be
linked without the Library, or if the work is itself a library. The
threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data
structure layouts and accessors, and small macros and small
inline
functions (ten lines or less in length), then the use of the object
file is unrestricted, regardless of whether it is legally a derivative
work. (Executables containing this object code plus portions of the
Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may
distribute the object code for the work under the terms of Section 6.
Any executables containing that work also fall under Section 6,
whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also compile or
link a "work that uses the Library" with the Library to produce a
work containing portions of the Library, and distribute that work
under terms of your choice, provided that the terms permit
modification of the work for the customer's own use and reverse
engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the
Library is used in it and that the Library
and its use are covered by
this License. You must supply a copy of this License. If the work

during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

c) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

d) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable
runs, unless that component itself accompanies
the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined

library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other

pertinent obligations, then as a consequence you
may not distribute the Library at all. For example, if a patent
license would not permit royalty-free redistribution of the Library by
all those who receive copies directly or indirectly through you, then
the only way you could satisfy both it and this License would be to
refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any
particular circumstance, the balance of the section is intended to apply,
and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any
patents or other property right claims or to contest validity of any
such claims; this section has the sole purpose of protecting the
integrity of the free software distribution system which is
implemented by public license practices. Many people have made
generous contributions to the wide range of software distributed
through that
system in reliance on consistent application of that
system; it is up to the author/donor to decide if he or she is willing
to distribute software through any other system and a licensee cannot
impose that choice.

This section is intended to make thoroughly clear what is believed to
be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in
certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Library under this License may add
an explicit geographical distribution limitation excluding those countries,
so that distribution is permitted only in or among countries not thus
excluded. In such case, this License incorporates the limitation as if
written in the body of this License.

13. The Free Software Foundation may publish revised and/or new
versions of the Library General Public License from time to time.
Such new versions will be similar in spirit to the present version,
but
may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library
specifies a version number of this License which applies to it and
"any later version", you have the option of following the terms and
conditions either of that version or of any later version published by
the Free Software Foundation. If the Library does not specify a
license version number, you may choose any version ever published by
the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or
modify it under the terms of the GNU Library General Public
License as published by the Free Software Foundation; either
version 2 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
Library General Public License for more details.

You should have received a copy of the GNU Library General Public
License along with this library; if not, write to the Free Software
Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer)
or your
school, if any, to sign a "copyright disclaimer" for the library, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the
library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

1.93 tar 1.29

1.93.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for

software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those

products. If such problems arise substantially in other domains, we stand
ready to extend this provision to those domains in future versions
of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and
"recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is

not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The
"System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally
available free
programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered
by this License only if the output, given its
content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed;
section 10
makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of

technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately
publish on each copy an appropriate copyright notice;
keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to
"keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution

medium, is called an
"aggregate" if the compilation and its resulting copyright are not
used to limit the access or legal rights of the compilation's users
beyond what the individual works permit. Inclusion of a covered work
in an aggregate does not cause this License to apply to the other
parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms
of sections 4 and 5, provided that you also convey the
machine-readable Corresponding Source under the terms of this License,
in one of these ways:

a) Convey the object code in, or embodied in, a physical product
(including a physical distribution medium), accompanied by the
Corresponding Source fixed on a durable physical medium
customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product
(including a physical distribution medium), accompanied by a
written offer, valid for at least three years
and valid for as
long as you offer spare parts or customer support for that product
model, to give anyone who possesses the object code either (1) a
copy of the Corresponding Source for all the software in the
product that is covered by this License, on a durable physical
medium customarily used for software interchange, for a price no
more than your reasonable cost of physically performing this
conveying of source, or (2) access to copy the
Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the
written offer to provide the Corresponding Source. This
alternative is allowed only occasionally and noncommercially, and
only if you received the object code with such an offer, in accord
with subsection 6b.

d) Convey the object code by offering access from a designated
place (gratis or for a charge), and offer equivalent access to the
Corresponding Source in
the same way through the same place at no
further charge. You need not require recipients to copy the
Corresponding Source along with the object code. If the place to
copy the object code is a network server, the Corresponding Source
may be on a different server (operated by you or a third party)
that supports equivalent copying facilities, provided you maintain
clear directions next to the object code saying where to find the

Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on

those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above
requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright
holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights
granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of

rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this

License will continue to apply to the part which is the covered work,
but the special requirements of the GNU Affero General Public License,
section 13, concerning interaction through a network will apply to the
combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of
the GNU General Public License from time to time. Such new versions will
be similar in spirit to the present version, but may differ in detail to
address new problems or concerns.

Each version is given a distinguishing version number. If the
Program specifies that a certain numbered version of the GNU General
Public License "or any later version" applies to it, you
have the
option of following the terms and conditions either of that numbered
version or of any later version published by the Free Software
Foundation. If the Program does not specify a version number of the
GNU General Public License, you may choose any version ever published
by the Free Software Foundation.

If the Program specifies that a proxy can decide which future
versions of the GNU General Public License can be used, that proxy's
public statement of acceptance of a version permanently authorizes you
to choose that version for the Program.

Later license versions may give you additional or different
permissions. However, no additional obligations are imposed on any
author or copyright holder as a result of your choosing to follow a
later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY
APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT
HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS"
WITHOUT WARRANTY
OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM
IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF
ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING
WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS

THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17.
Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>
This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what you want to
do, use the GNU Lesser General
Public License instead of this License. But first, please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.

1.94 perl 5.22.1

1.94.1 Available under license :

The "Artistic License"

Preamble

The intent of this document is to state the conditions under which a
Package may be copied, such that the Copyright Holder maintains some
semblance of artistic control over the development of the package,
while giving the users of the package the right to use and distribute
the Package in a more-or-less customary fashion, plus the right to make
reasonable modifications.

Definitions:

"Package" refers to the collection of files distributed by the
Copyright Holder, and derivatives of that collection of files
created through textual modification.

"Standard Version" refers to such a Package if it has not been
modified, or has been modified in accordance with the wishes
of the Copyright Holder as specified below.

"Copyright Holder" is whoever is named in the copyright or
copyrights for the package.

"You" is you, if you're thinking
about copying or distributing
this Package.

"Reasonable copying fee" is whatever you can justify on the
basis of media cost, duplication charges, time of people involved,
and so on. (You will not be required to justify it to the
Copyright Holder, but only to the computing community at large
as a market that must bear the fee.)

"Freely Available" means that no fee is charged for the item
itself, though there may be fees involved in handling the item.
It also means that recipients of the item may redistribute it
under the same conditions they received it.

1. You may make and give away verbatim copies of the source form of the
Standard Version of this Package without restriction, provided that you
duplicate all of the original copyright notices and associated disclaimers.

2. You may apply bug fixes, portability fixes and other modifications
derived from the Public Domain or from the Copyright Holder.
A Package
modified in such a way shall still be considered the Standard Version.

3. You may otherwise modify your copy of this Package in any way, provided
that you insert a prominent notice in each changed file stating how and
when you changed that file, and provided that you do at least ONE of the
following:

a) place your modifications in the Public Domain or otherwise make them
Freely Available, such as by posting said modifications to Usenet or
an equivalent medium, or placing the modifications on a major archive
site such as uunet.uu.net, or by allowing the Copyright Holder to include
your modifications in the Standard Version of the Package.

b) use the modified Package only within your corporation or organization.

c) rename any non-standard executables so the names do not conflict with standard executables, which must also be provided, and provide a separate manual page for each non-standard executable that clearly documents how it
differs from the Standard Version.

d) make other distribution arrangements with the Copyright Holder.

4. You may distribute the programs of this Package in object code or executable form, provided that you do at least ONE of the following:

a) distribute a Standard Version of the executables and library files, together with instructions (in the manual page or equivalent) on where to get the Standard Version.

b) accompany the distribution with the machine-readable source of the Package with your modifications.

c) give non-standard executables non-standard names, and clearly document the differences in manual pages (or equivalent), together with instructions on where to get the Standard Version.

d) make other distribution arrangements with the Copyright Holder.

5. You may charge a reasonable copying fee for any distribution of this Package. You may charge any fee you choose for support of this Package. You may not charge a fee for this Package
itself. However,
you may distribute this Package in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution provided that you do not advertise this Package as a product of your own. You may embed this Package's interpreter within an executable of yours (by linking); this shall be construed as a mere form of aggregation, provided that the complete Standard Version of the interpreter is so embedded.

6. The scripts and library files supplied as input to or produced as output from the programs of this Package do not automatically fall under the copyright of this Package, but belong to whoever generated them, and may be sold commercially, and may be aggregated with this Package. If such scripts or library files are aggregated with this Package via the so-called "undump" or "unexec" methods of producing a binary executable image, then distribution of such an image shall neither be construed as a distribution of this Package
nor shall it
fall under the restrictions of Paragraphs 3 and 4, provided that you do not represent such an executable image as a Standard Version of this

Package.

7. C subroutines (or comparably compiled subroutines in other
languages) supplied by you and linked into this Package in order to
emulate subroutines and variables of the language defined by this
Package shall not be considered part of this Package, but are the
equivalent of input as in Paragraph 6, provided these subroutines do
not change the language in any way that would cause it to fail the
regression tests for the language.

8. Aggregation of this Package with a commercial distribution is always
permitted provided that the use of this Package is embedded; that is,
when no overt attempt is made to make this Package's interfaces visible
to the end user of the commercial distribution. Such use shall not be
construed as a distribution of this Package.

9. The name of the Copyright Holder may not be used to endorse or promote
products
 derived from this software without specific prior written permission.

10. THIS PACKAGE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The End

---
abstract: 'Build and install Perl modules'
author:
 - 'Ken Williams <kwilliams@cpan.org>'
 - "Development questions, bug reports, and patches should be sent to the\nModule-Build mailing list at <module-build@perl.org>."
build_requires:
 File::Temp: 0.15
 Test::Harness: 3.16
 Test::More: 0.49
generated_by: 'Module::Build version 0.3608'
license: gpl
meta-spec:
 url: http://module-build.sourceforge.net/META-spec-v1.4.html
 version: 1.4
name: Module-Build
resources:
 MailingList: mailto:module-build@perl.org
 license: http://dev.perl.org/licenses/
 repository: http://github.com/dagolden/module-build/
version: 3

This program, "bzip2", the associated library "libbzip2", and all documentation, are copyright (C) 1996-2010 Julian R Seward. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

3. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

4. The name of the author may not be used to endorse or promote products derived from this software without specific
prior written
permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Julian Seward, jseward@bzip.org
bzip2/libbzip2 version 1.0.6 of 6 September 2010

GNU GENERAL PUBLIC LICENSE
Version 1, February 1989

Copyright (C) 1989 Free Software Foundation, Inc.
51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The license agreements of most software companies try to keep users at the mercy of those companies. By contrast, our General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. The General Public License applies to the Free Software Foundation's software and to any other program whose authors commit to using it. You can use it for your programs, too.

When we speak of free software, we are referring to freedom, not price. Specifically, the General Public License is designed to make sure that you have the freedom to
give away or sell copies of free
software, that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of a such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must tell them their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that
everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any work containing the Program or a portion of it, either verbatim or with modifications. Each licensee is addressed as "you".

1. You may copy and distribute verbatim
copies of the Program's source
code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this General Public License and to the absence of any warranty; and give any other recipients of the Program a copy of this General Public License along with the Program. You may charge a fee for the physical act of transferring a copy.

2. You may modify your copy or copies of the Program or any portion of it, and copy and distribute such modifications under the terms of Paragraph 1 above, provided that you also do the following:

a) cause the modified files to carry prominent notices stating that you changed the files and the date of any change; and

b) cause the whole of any work that you distribute or publish, that in whole or in part contains the Program or any part thereof, either with or without modifications, to be licensed
at no charge to all
third parties under the terms of this General Public License (except that you may choose to grant warranty protection to some or all third parties, at your option).

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the simplest and most usual way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this General Public License.

d) You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

Mere aggregation of another independent work with the Program (or its

derivative) on a volume of a storage or distribution medium
does not bring
the other work under the scope of these terms.

3. You may copy and distribute the Program (or a portion or derivative of it, under Paragraph 2) in object code or executable form under the terms of Paragraphs 1 and 2 above provided that you also do one of the following:

a) accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Paragraphs 1 and 2 above; or,

b) accompany it with a written offer, valid for at least three years, to give any third party free (except for a nominal charge for the cost of distribution) a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Paragraphs 1 and 2 above; or,

c) accompany it with the information you received as to where the corresponding source code may be obtained. (This alternative is allowed only for noncommercial distribution and only if you received the program
in object code or executable form alone.)

Source code for a work means the preferred form of the work for making modifications to it. For an executable file, complete source code means all the source code for all modules it contains; but, as a special exception, it need not include source code for modules which are standard libraries that accompany the operating system on which the executable file runs, or for standard header files or definitions files that accompany that operating system.

4. You may not copy, modify, sublicense, distribute or transfer the Program except as expressly provided under this General Public License. Any attempt otherwise to copy, modify, sublicense, distribute or transfer the Program is void, and will automatically terminate your rights to use the Program under this License. However, parties who have received copies, or rights to use copies, from you under this General Public License will not have their licenses terminated so long as such parties remain
in full compliance.

5. By copying, distributing or modifying the Program (or any work based on the Program) you indicate your acceptance of this license to do so, and all its terms and conditions.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original

licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein.

7. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of the license which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the license, you may choose any version ever published by the Free Software Foundation.

8. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

9. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

10. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Appendix: How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to humanity, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) 19yy <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 1, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19xx name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show

c'; they could even be mouse-clicks or menu items--whatever suits your
program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here a sample; alter the names:

 Yoyodyne, Inc., hereby disclaims all copyright interest in the
 program `Gnomovision' (a program to direct compilers to make passes
 at assemblers) written by James Hacker.

 <signature of Ty Coon>, 1 April 1989
 Ty Coon, President of Vice

That's all there is to it!
#!perl

=head1 NAME

copyright.t

=head1 DESCRIPTION

Tests that the latest copyright years in the top-level README file and the
C<perl -v> output match each other.

If the test fails, update at least one of README and perl.c so that they match
reality.

Optionally you can pass the C<--now> option to check they are at the current
year. This isn't checked by default, so that it doesn't fail for people
working on older releases. It should be run before making a new release.

=cut

use strict;
use Config;
BEGIN { require './test.pl' }

if ($Config{usecrosscompile}) {
 skip_all("Not all files are available during cross-compilation");
}

my ($opt) = @ARGV;

my $readme_year = readme_year();
my $v_year = v_year();

```
# Check that both copyright dates are up-to-date, but only if requested, so
# that tests still pass for people intentionally working on older versions:
if ($opt eq '--now')
{
 my $current_year = (gmtime)[5] + 1900;
 is $v_year, $current_year, 'perl -v copyright includes current
 year';
 is $readme_year, $current_year, 'README copyright includes current year';
}

# Otherwise simply check that the two copyright dates match each other:
else
{
 is $readme_year, $v_year, 'README and perl -v copyright dates match';
}

done_testing;



sub readme_year
# returns the latest copyright year from the top-level README file
{

 open my $readme, '<', '../README' or die "Opening README failed: $!";

 # The copyright message is the first paragraph:
 local $/ = '';
 my $copyright_msg = <$readme>;

 my ($year) = $copyright_msg =~ /.*\b(\d{4,})/s
    or die "Year not found in README copyright message '$copyright_msg'";

 $year;
}



sub v_year
# returns the latest copyright year shown in perl -v
{

 my $output = runperl switches => ['-v'];
 my ($year) = $output =~ /copyright 1987.*\b(\d{4,})/i
    or die "Copyright statement not found in perl -v output '$output'";

 $year;
}
This software is copyright (c) 2017 by Ken Williams.
```

This is free software; you can redistribute it and/or modify it under
the same terms as the Perl 5 programming language system itself.

Terms of the Perl programming language system itself

a) the GNU General Public License as published by the Free
  Software Foundation; either version 1, or (at your option) any
  later version, or
b) the "Artistic License"

--- The GNU General Public License, Version 1, February 1989 ---

This software is Copyright (c) 2017 by Ken Williams.

This is free software, licensed under:

 The GNU General Public License, Version 1, February 1989

                GNU GENERAL PUBLIC LICENSE
                 Version 1, February 1989

Copyright (C) 1989 Free Software Foundation, Inc.
51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

                     Preamble

  The license agreements of most software companies try to keep users
at the mercy of those companies. By contrast, our General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. The
General Public License applies to the Free Software Foundation's
software and to any other program whose authors commit to using it.
You can use it for your programs, too.

 When we speak of free software, we are referring to freedom, not
price. Specifically, the General Public License is designed to make
sure that you have the freedom to give away or sell copies of free
software, that you receive source code or can get it if you want it,
that you can change the software or use pieces of it in new free
programs; and that you know you can do these things.

 To protect your rights, we need to make restrictions that forbid
anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate

to certain responsibilities for you if you
distribute copies of the software, or if you modify it.

For example, if you distribute copies of a such a program, whether
gratis or for a fee, you must give the recipients all the rights that
you have. You must make sure that they, too, receive or can get the
source code. And you must tell them their rights.

We protect your rights with two steps: (1) copyright the software, and
(2) offer you this license which gives you legal permission to copy,
distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain
that everyone understands that there is no warranty for this free
software. If the software is modified by someone else and passed on, we
want its recipients to know that what they have is not the original, so
that any problems introduced by others will not reflect on the original
authors' reputations.

The precise terms and conditions for copying, distribution and
modification
follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any program or other work which
contains a notice placed by the copyright holder saying it may be
distributed under the terms of this General Public License. The
"Program", below, refers to any such program or work, and a "work based
on the Program" means either the Program or any work containing the
Program or a portion of it, either verbatim or with modifications. Each
licensee is addressed as "you".

1. You may copy and distribute verbatim copies of the Program's source
code as you receive it, in any medium, provided that you conspicuously and
appropriately publish on each copy an appropriate copyright notice and
disclaimer of warranty; keep intact all the notices that refer to this
General Public License and to the absence of any warranty; and give any
other recipients of the Program a copy of this General Public License
along
with the Program. You may charge a fee for the physical act of
transferring a copy.

2. You may modify your copy or copies of the Program or any portion of
it, and copy and distribute such modifications under the terms of Paragraph
1 above, provided that you also do the following:

a) cause the modified files to carry prominent notices stating that you changed the files and the date of any change; and

b) cause the whole of any work that you distribute or publish, that in whole or in part contains the Program or any part thereof, either with or without modifications, to be licensed at no charge to all third parties under the terms of this General Public License (except that you may choose to grant warranty protection to some or all third parties, at your option).

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the simplest and most
usual way, to print or display an
announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this General Public License.

d) You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

Mere aggregation of another independent work with the Program (or its derivative) on a volume of a storage or distribution medium does not bring the other work under the scope of these terms.

3. You may copy and distribute the Program (or a portion or derivative of it, under Paragraph 2) in object code or executable form under the terms of Paragraphs 1 and 2 above provided that you also do one of the following:

a) accompany it with the complete corresponding machine-readable source code, which
must be distributed under the terms of
Paragraphs 1 and 2 above; or,

b) accompany it with a written offer, valid for at least three years, to give any third party free (except for a nominal charge for the cost of distribution) a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Paragraphs 1 and 2 above; or,

c) accompany it with the information you received as to where the corresponding source code may be obtained. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form alone.)

Source code for a work means the preferred form of the work for making modifications to it. For an executable file, complete source code means all the source code for all modules it contains; but, as a special exception, it need not include source code for modules which are standard libraries that accompany the operating system on which the executable file runs, or for standard header files or definitions files that accompany that operating system.

4. You may not copy, modify, sublicense, distribute or transfer the Program except as expressly provided under this General Public License. Any attempt otherwise to copy, modify, sublicense, distribute or transfer the Program is void, and will automatically terminate your rights to use the Program under this License. However, parties who have received copies, or rights to use copies, from you under this General Public License will not have their licenses terminated so long as such parties remain in full compliance.

5. By copying, distributing or modifying the Program (or any work based on the Program) you indicate your acceptance of this license to do so, and all its terms and conditions.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein.

7. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of the license which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the license, you may choose any version ever published by the Free Software Foundation.

8. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals

of preserving the free status of all derivatives of our free software and
of promoting the sharing and reuse of software generally.

NO WARRANTY

9. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

10. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Appendix: How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to humanity, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program.
It is safest to
attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) 19yy <name of author>

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation; either version 1, or (at your option)
any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 51 Franklin
Street, Fifth Floor, Boston MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19xx name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the
appropriate parts of the General Public License. Of course, the
commands you use may be called something other than `show w' and `show
c'; they could even be mouse-clicks or menu items--whatever suits your
program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here a sample; alter the names:

Yoyodyne, Inc., hereby disclaims
all copyright interest in the
program `Gnomovision' (a program to direct compilers to make passes
at assemblers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

That's all there is to it!

--- The Artistic License 1.0 ---

This software is Copyright (c) 2017 by Ken Williams.

This is free software, licensed under:

The Artistic License 1.0

The Artistic License

Preamble

The intent of this document is to state the conditions under which a Package may be copied, such that the Copyright Holder maintains some semblance of artistic control over the development of the package, while giving the users of the package the right to use and distribute the Package in a more-or-less customary fashion, plus the right to make reasonable modifications.

Definitions:

- "Package" refers to the collection of files distributed by the Copyright Holder, and derivatives of that collection of files created through textual modification.

- "Standard Version" refers to such a Package if it has not been modified, or has been modified in accordance with the wishes of the Copyright Holder.
- "Copyright Holder" is whoever is named in the copyright or copyrights for the package.
- "You" is you, if you're thinking about copying or distributing this Package.
- "Reasonable copying fee" is whatever you can justify on the basis of media cost, duplication charges, time of people involved, and so on. (You will not be required to justify it to the Copyright Holder, but only to the computing community at large as a market that must bear the fee.)
- "Freely Available" means that no fee is charged for the item itself, though there may be fees involved in handling the item. It also means that recipients of the item may redistribute it under the same conditions they received it.

1. You may make and give away verbatim copies of the source form of the Standard Version of this Package without
restriction, provided that you
duplicate all of the original copyright notices and associated disclaimers.

2. You may apply bug fixes, portability fixes and other modifications derived from the Public Domain or from the Copyright Holder. A Package modified in such a way shall still be considered the Standard Version.

3. You may otherwise modify your copy of this Package in any way, provided that you insert a prominent notice in each changed file stating how and when you changed that file, and provided that you do at least ONE of the following:

a) place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an

equivalent medium, or placing the modifications on a major archive site such as ftp.uu.net, or by allowing the Copyright Holder to include your modifications in the Standard Version of the Package.

b) use the modified Package only within your corporation or organization.

c)
rename any non-standard executables so the names do not conflict with standard executables, which must also be provided, and provide a separate manual page for each non-standard executable that clearly documents how it differs from the Standard Version.

d) make other distribution arrangements with the Copyright Holder.

4. You may distribute the programs of this Package in object code or executable form, provided that you do at least ONE of the following:

a) distribute a Standard Version of the executables and library files, together with instructions (in the manual page or equivalent) on where to get the Standard Version.

b) accompany the distribution with the machine-readable source of the Package with your modifications.

c) accompany any non-standard executables with their corresponding Standard Version executables, giving the non-standard executables non-standard names, and clearly documenting the differences in manual pages (or equivalent), together with instructions on where to get the Standard Version.

d) make other distribution arrangements with the Copyright Holder.

5. You may charge a reasonable copying fee for any distribution of this Package. You may charge any fee you choose for support of this Package. You may not charge a fee for this Package itself. However, you may distribute this Package in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution provided that you do not advertise this Package as a product of your own.

6. The scripts and library files supplied as input to or produced as output from the programs of this Package do not automatically fall under the copyright of this Package, but belong to whomever generated them, and may be sold commercially, and may be aggregated with this Package.

7. C or perl subroutines supplied by you and linked into this Package shall not be considered part of this Package.

8. The name

of the Copyright Holder may not be used to endorse or promote
products derived from this software without specific prior written permission.

9. THIS PACKAGE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The End
GNU AFFERO GENERAL PUBLIC LICENSE
Version 3, 19 November 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU Affero General Public License is a free, copyleft license for software and other kinds of works, specifically designed to ensure cooperation with the community in the case of network server software.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works.
By contrast,
our General Public Licenses are intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

Developers that use our General Public Licenses protect your rights with two
steps: (1) assert copyright on the software, and (2) offer
you this License which gives you legal permission to copy, distribute and/or modify the software.

A secondary benefit of defending all users' freedom is that improvements made in alternate versions of the program, if they receive widespread use, become available for other developers to incorporate. Many developers of free software are heartened and encouraged by the resulting cooperation. However, in the case of software used on network servers, this result may fail to come about.
The GNU General Public License permits making a modified version and

letting the public access it on a server without ever releasing its source code to the public.

The GNU Affero General Public License is designed specifically to ensure that, in such cases, the modified source code becomes available to the community. It requires the operator of a network server to provide the source code of the modified version running there to the users of that server. Therefore, public use of a modified version, on a publicly accessible server, gives the public access to the source code of the modified version.

An older license, called the Affero General Public License and published by Affero, was designed to accomplish similar goals. This is a different license, not a version of the Affero GPL, but Affero has released a new version of the Affero GPL which permits relicensing under this license.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU Affero General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying,

distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License,
and how to view a copy of this License. If
the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System
Libraries" of an executable work include anything, other
than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form
means all
the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but

which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts
of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its

content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit
them from making any copies of
your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such

measures.

When you convey a covered
work, you waive any legal power to forbid
circumvention of technological measures to the extent such circumvention
is effected by exercising rights under this License with respect to
the covered work, and you disclaim any intention to limit operation or
modification of the work as a means of enforcing, against the work's
users, your or third parties' legal rights to forbid circumvention of
technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you
receive it, in any medium, provided that you conspicuously and
appropriately publish on each copy an appropriate copyright notice;
keep intact all notices
stating that this License and any
non-permissive terms added in accord with section 7 apply to the code;
keep intact all notices of the absence of any warranty; and give all
recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey,
and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to
produce it from the Program, in the form of source code under the
terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent
notices stating that you modified
it, and giving a relevant date.

b) The work must carry prominent notices stating that it is
released under this License and any conditions added under section
7. This requirement modifies the requirement in section 4 to
"keep intact all notices".

c) You must license the entire work, as a whole, under this
License to anyone who comes into possession of a copy. This
License will therefore apply, along with any applicable section 7
additional terms, to the whole of the work, and all its parts,
regardless of how they are packaged. This License gives no
permission to license the work
in any other way, but it does not
invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not

used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding
Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this

conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated
place (gratis or for a charge), and offer equivalent access to the
Corresponding Source in the same way through the same place at no
further charge. You need not require recipients to copy the

Corresponding Source along with the object code. If the place to
copy the object code is a network server, the Corresponding Source
may be on a different server (operated by you or a third party)
that supports equivalent copying facilities, provided you maintain
clear directions next to the object code saying where to find the
Corresponding Source. Regardless of what server hosts the
Corresponding Source, you remain obligated to ensure that it is
available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided
you inform other peers where the object code and Corresponding
Source of the work are being
offered to the general public at no
charge under subsection 6d.

A separable portion of the object code, whose source code is excluded
from the Corresponding Source as a System Library, need not be
included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any
tangible personal property which is normally used for personal, family,
or household purposes, or (2) anything designed or sold for incorporation
into a dwelling. In determining whether a product is a consumer product,
doubtful cases shall be resolved in favor of coverage. For a particular
product received by a particular user, "normally used" refers to a

typical or common use of that class of product, regardless of the status
of the particular user or of the way in which the particular user
actually uses, or expects or is expected to use, the product. A product
is a consumer product regardless of whether the product has substantial
commercial, industrial or non-consumer uses, unless such uses represent
the only significant mode of use of the product.

"Installation Information" for a User Product means any methods,
procedures, authorization keys, or other information required to install
and execute modified versions of a covered work in that User Product from
a modified version of its Corresponding Source. The information must
suffice to ensure that the continued
functioning of the modified object
code is in no case prevented or interfered with solely because
modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object
code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly

documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by

this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of

that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining
to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further

restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated
as exceptions;
the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright

holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently

reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever

licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing
the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For

purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license

to a
party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly
relying" means you have
actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work
and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work

conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Remote Network Interaction; Use with the GNU General Public License.

Notwithstanding any other provision of this License, if you modify the Program, your modified version must prominently offer all users interacting with it remotely through a computer network (if your version supports such interaction) an opportunity to receive the Corresponding Source of your version by providing access to the Corresponding Source from a network server at no charge, through some standard or customary means of facilitating copying of software. This Corresponding Source shall include the Corresponding Source for any work covered by version 3 of the GNU General Public License that is incorporated pursuant to the following paragraph.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU General Public License into a single

combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the work with which it is combined will remain governed by version 3 of the GNU General Public License.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU Affero General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU Affero General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered

version or of any later version published by the Free Software
Foundation. If the Program does not specify a version number of the
GNU Affero General Public License, you may choose any version ever published
by the Free Software Foundation.

If the Program specifies that a proxy can decide which future
versions of the GNU Affero General Public License can be used, that proxy's
public statement of acceptance of a version permanently authorizes you
to choose that version for the Program.

Later license versions
may give you additional or different
permissions. However, no additional obligations are imposed on any
author or copyright holder as a result of your choosing to follow a
later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY
APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT
HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY

OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR

PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM

IS WITH YOU. SHOULD
THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF
ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING
WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS

THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY

GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE

USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF

DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD

PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS),

EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED

OF THE POSSIBILITY OF
SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided
above cannot be given local legal effect according to their terms,
reviewing courts shall apply local law that most closely approximates
an absolute waiver of all civil liability in connection with the
Program, unless a warranty or assumption of liability accompanies a
copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program,
and you want it to be of the greatest
possible use to the public, the best way to achieve this is to make it
free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest
to attach them to the start of each source file to most effectively
state the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify
it under
the terms of the GNU Affero General Public License as published by
the Free Software Foundation, either version 3 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU Affero General Public License for more details.

You should have received a copy of the GNU Affero General Public License
along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If your software can interact with users remotely through a computer
network, you should also make sure that it provides a way for users to

get its source. For example, if your program is a web application, its
interface could display a "Source" link that leads users to an archive
of the code. There are many ways you could offer source, and different
solutions will be better for different programs; see section 13 for the
specific requirements.

 You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU AGPL, see
<http://www.gnu.org/licenses/>.

1.95 tcpdump 4.7.4

1.95.1 Available under license :

License: BSD

Redistribution and use in source and binary forms, with or without

modification, are permitted provided that the following conditions
are met:

1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in
   the documentation and/or other materials provided with the
   distribution.
3. The names of the authors may not be used to endorse or promote
   products derived from this software without specific prior
   written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

1.96 xz 5.2.2

1.96.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it. (Some other Free Software Foundation software is covered by
the GNU Lesser General Public License instead.) You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price.
Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which
gives you legal permission to copy,
distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of

running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you

distribute the same sections as part of a whole which is a work based
on the Program, the distribution of the whole must be on the terms of
this License, whose permissions for other licensees extend to the
entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest
your rights to work written entirely by you; rather, the intent is to
exercise the right to control the distribution of derivative or
collective works based on the Program.

In addition, mere aggregation of another work not based on the Program
with the Program (or with a work based on the Program) on a volume of
a storage or distribution medium does not bring the other work under
the scope of this License.

3. You may copy and distribute the Program (or a work based on it,
under Section 2) in object code or executable form under the terms of
Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable
source code, which must be distributed under the terms of Sections
1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three
years, to give any third party, for a charge no more than your
cost of physically performing source distribution, a complete
machine-readable copy of the corresponding source code, to be
distributed under the terms of Sections 1 and 2 above on a medium
customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer
to distribute corresponding source code. (This alternative is
allowed only for noncommercial distribution
and only if you
received the program in object code or executable form with such
an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for
making modifications to it. For an executable work, complete source
code means all the source code for all modules it contains, plus any
associated interface definition files, plus the scripts used to
control compilation and installation of the executable. However, as a
special exception, the source code distributed need not include
anything that is normally distributed (in either source or binary
form) with the major components (compiler, kernel, and so on) of the
operating system on which the executable runs, unless that component
itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under

any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE,
THERE IS NO WARRANTY
FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR
THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU
General Public License as published by
the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful,

but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License along
with this program; if not, write to the Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute
it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this
is what you want to do, use the GNU Lesser General
Public License instead of this License.

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for
software and other kinds of works.

The licenses for most software and other practical works are designed
to take away your freedom to share and change the works. By contrast,
the GNU General Public License is intended to guarantee your freedom to
share and change all versions of a program--to make sure it remains free
software for all its users. We, the Free Software Foundation, use the
GNU General Public License for most of our software; it applies also to
any other work released this way by its authors. You can apply it to
your programs, too.

When we speak of free software, we are referring to
freedom, not
price. Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
them if you wish), that you receive source code or can get it if you
want it, that you can change the software or use pieces of it in new
free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you
these rights or asking you to surrender the rights. Therefore, you have
certain responsibilities if you distribute copies of the software, or if
you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether
gratis or for a fee, you must pass on to the recipients the same
freedoms that you received. You must make sure that they, too, receive
or can get the source code. And you must show them these terms so they
know their rights.

Developers that use the GNU GPL protect your rights with two steps:
(1)
assert copyright on the software, and (2) offer you this License
giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains
that there is no warranty for this free software. For both users' and
authors' sake, the GPL requires that modified versions be marked as
changed, so that their problems will not be attributed erroneously to
authors of previous versions.

Some devices are designed to deny users access to install or run
modified versions of the software inside them, although the manufacturer
can do so. This is fundamentally incompatible with the aim of
protecting users' freedom to change the software. The systematic
pattern of such abuse occurs in the area of products for individuals to

use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand
ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees"
and
"recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through

a computer network, with no transfer of a copy, is
not conveying.

An interactive user interface displays "Appropriate Legal Notices"
to the extent that it includes a convenient and prominently visible
feature that (1) displays an appropriate copyright notice, and (2)
tells the user that there is no warranty for the work (except to the
extent that warranties are provided), that licensees may convey the
work under this License, and how to view a copy of this License. If
the interface presents a list of user commands or options, such as a
menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work
for making modifications to it. "Object code" means any non-source
form of a work.

A "Standard Interface" means an interface that either is an official
standard defined by a recognized standards body, or, in the case of
interfaces specified for a particular programming language, one that
is widely used among developers working in that language.

The
"System Libraries" of an executable work include anything, other
than the work as a whole, that (a) is included in the normal form of
packaging a Major Component, but which is not part of that Major
Component, and (b) serves only to enable use of the work with that
Major Component, or to implement a Standard Interface for which an
implementation is available to the public in source code form. A
"Major Component", in this context, means a major essential component
(kernel, window system, and so on) of the specific operating system
(if any) on which the executable work runs, or a compiler used to
produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all
the source code needed to generate, install, and (for an executable
work) run the object code and to modify the work, including scripts to
control those activities. However, it does not include the work's
System Libraries, or general-purpose tools or generally
available free
programs which are used unmodified in performing those activities but
which are not part of the work. For example, Corresponding Source
includes interface definition files associated with source files for
the work, and the source code for shared libraries and dynamically
linked subprograms that the work is specifically designed to require,
such as by intimate data communication or control flow between those
subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered
by this License only if the output, given its
content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed;
section 10
makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's

users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately
publish on each copy an appropriate copyright notice;
keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program,

in or on a volume of a storage or distribution
medium, is called an
"aggregate" if the compilation and its resulting copyright are not
used to limit the access or legal rights of the compilation's users
beyond what the individual works permit. Inclusion of a covered work
in an aggregate does not cause this License to apply to the other
parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms
of sections 4 and 5, provided that you also convey the
machine-readable Corresponding Source under the terms of this License,
in one of these ways:

a) Convey the object code in, or embodied in, a physical product
(including a physical distribution medium), accompanied by the
Corresponding Source fixed on a durable physical medium
customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product
(including a physical distribution medium), accompanied by a
written offer, valid for at least three years
and valid for as
long as you offer spare parts or customer support for that product
model, to give anyone who possesses the object code either (1) a
copy of the Corresponding Source for all the software in the
product that is covered by this License, on a durable physical
medium customarily used for software interchange, for a price no
more than your reasonable cost of physically performing this
conveying of source, or (2) access to copy the
Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the
written offer to provide the Corresponding Source. This
alternative is allowed only occasionally and noncommercially, and
only if you received the object code with such an offer, in accord
with subsection 6b.

d) Convey the object code by offering access from a designated
place (gratis or for a charge), and offer equivalent access to the
Corresponding Source in
the same way through the same place at no
further charge. You need not require recipients to copy the
Corresponding Source along with the object code. If the place to
copy the object code is a network server, the Corresponding Source
may be on a different server (operated by you or a third party)
that supports equivalent copying facilities, provided you maintain

clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in

ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or

requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on

those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above
requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright

holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright
holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights

granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work

in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed

under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17.
Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License

along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>
This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what you want to
do, use the GNU Lesser General
Public License instead of this License. But first, please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.

XZ Utils Licensing
==========

Different licenses apply to different files in this package. Here
is a rough summary of which licenses apply to which parts of this
package (but check the individual files to be sure!):

- liblzma is in the public domain.

- xz, xzdec, and lzmadec command line tools are in the public
domain unless GNU getopt_long had to be compiled and linked
in from the lib directory. The getopt_long code is under
GNU LGPLv2.1+.

- The scripts to grep, diff, and view compressed files have been
adapted from gzip. These scripts and their documentation are
under GNU GPLv2+.

- All the documentation in the doc directory and most of the
  XZ Utils specific documentation files in other directories
  are in the public domain.

- Translated messages are in the public domain.

- The build system contains public domain files, and files that
  are under GNU GPLv2+ or GNU
GPLv3+. None of these files end up
  in the binaries being built.

- Test files and test code in the tests directory, and debugging
  utilities in the debug directory are in the public domain.

- The extra directory may contain public domain files, and files
  that are under various free software licenses.

You can do whatever you want with the files that have been put into
the public domain. If you find public domain legally problematic,
take the previous sentence as a license grant. If you still find
the lack of copyright legally problematic, you have too many
lawyers.

As usual, this software is provided "as is", without any warranty.

If you copy significant amounts of public domain code from XZ Utils
into your project, acknowledging this somewhere in your software is
polite (especially if it is proprietary, non-free software), but
naturally it is not legally required. Here is an example of a good
notice to
put into "about box" or into documentation:

    This software includes code from XZ Utils <https://tukaani.org/xz/>.

The following license texts are included in the following files:
- COPYING.LGPLv2.1: GNU Lesser General Public License version 2.1
- COPYING.GPLv2: GNU General Public License version 2
- COPYING.GPLv3: GNU General Public License version 3

Note that the toolchain (compiler, linker etc.) may add some code
pieces that are copyrighted. Thus, it is possible that e.g. liblzma
binary wouldn't actually be in the public domain in its entirety
even though it contains no copyrighted code from the XZ Utils source
package.

If you have questions, don't hesitate to ask the author(s) for more
information.

1.97 at 3.1.20

1.97.1 Available under license :

This is the Debian GNU/Linux prepackaged version of the deferred
execution scheduler called at.

This package was debianized by its author Thomas Koenig
<ig25@rz.uni-karlsruhe.de>, taken over and re-packaged first by Martin
Schulze <joey@debian.org> and then by Siggy Brentrup <bsb@winnegan.de>,
and then taken over by Ryan Murray <rmurray@debian.org>.

In August 2009 the upstream development and Debian packaging were taken over
by Ansgar Burchardt <ansgar@debian.org> and Cyril Brulebois <kibi@debian.org>.

In August 2015 the upstream development and Debian packaging were
taken over by Jose M Calhariz <jose@calhariz.com>

This may be considered the experimental upstream source, and since there
doesn't seem to be any other upstream source, the only upstream source.

Copyright: 1993, 1994, 1995, 1996, 1997 (c) Thomas Koenig
1993 (c) David Parsons
2002, 2005 (c) Ryan Murray

This program is free software; you can redistribute it and/or modify
it under the terms
of the GNU General Public License as published by
the Free Software Foundation; either version 2 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

The files posixtm.c and posixtm.h have the following copyright information:

Copyright (C) 1989, 1990, 1991, 1998, 2000, 2001, 2002, 2003, 2004,
2005, 2006, 2007 Free Software Foundation Inc.

This program is free software: you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation; either version 3 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,

but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY
or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

parsetime.pl:

Copyright (C) 2009, Ansgar Burchardt <ansgar@debian.org>

Permission to use, copy, modify, and/or distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR
OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

On Debian GNU/Linux systems, the complete text of the GNU General
Public License can be found in `/usr/share/common-licenses/GPL'.
GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it. (Some other Free Software Foundation software is covered by
the GNU Library General Public License instead.) You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price. Our General Public Licenses are designed to
make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it

if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid
anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate to certain responsibilities for you if you
distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether
gratis or for a fee, you must give the recipients all the rights that
you have. You must make sure that they, too, receive or can get the
source code. And you must show them these terms so they know their
rights.

We protect your rights with two steps: (1) copyright the software, and
(2) offer you this license which gives you legal permission to copy,
distribute
and/or modify the software.

Also, for each author's protection and ours, we want to make certain
that everyone understands that there is no warranty for this free
software. If the software is modified by someone else and passed on, we
want its recipients to know that what they have is not the original, so
that any problems introduced by others will not reflect on the original
authors' reputations.

Finally, any free program is threatened constantly by software
patents. We wish to avoid the danger that redistributors of a free
program will individually obtain patent licenses, in effect making the
program proprietary. To prevent this, we have made it clear that any
patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and
modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which
contains
a notice placed by the copyright holder saying it may be distributed
under the terms of this General Public License. The "Program", below,
refers to any such program or work, and a "work based on the Program"
means either the Program or any derivative work under copyright law:
that is to say, a work containing the Program or a portion of it,
either verbatim or with modifications and/or translated into another
language. (Hereinafter, translation is included without limitation in
the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered

independent and separate works in
themselves, then this License, and its terms, do not apply to those
sections when you distribute them as separate works. But when you
distribute the same sections as part of a whole which is a work based
on the Program, the distribution of the whole must be on the terms of
this License, whose permissions for other licensees extend to the
entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest
your rights to work written entirely by you; rather, the intent is to
exercise the right to control the distribution of derivative or
collective works based on the Program.

In addition, mere aggregation of another work not based on the Program
with the Program (or with a work based on the Program) on a volume of
a storage or distribution medium does not bring the other work under
the scope of this License.

3. You may copy and distribute the Program (or a work based on
it,
under Section 2) in object code or executable form under the terms of
Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable
source code, which must be distributed under the terms of Sections
1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three
years, to give any third party, for a charge no more than your
cost of physically performing source distribution, a complete
machine-readable copy of the corresponding source code, to be
distributed under the terms of Sections 1 and 2 above on a medium
customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer
to distribute corresponding source code. (This alternative is
allowed only for noncommercial distribution and only if you
received the program in object code or executable
form with such
an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for
making modifications to it. For an executable work, complete source
code means all the source code for all modules it contains, plus any
associated interface definition files, plus the scripts used to
control compilation and installation of the executable. However, as a
special exception, the source code distributed need not include
anything that is normally distributed (in either source or binary

form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the
source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time
you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution
of the Program by
all those who receive copies directly or indirectly through you, then

the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free

Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN
IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License,

or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and
`show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this is what you want to do, use the GNU Library General
Public License instead of this License.

1.98 libvirt 1.3.5

1.98.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it. (Some other Free Software Foundation software is covered by
the GNU Lesser General Public License instead.) You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price.
Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid
anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate to certain responsibilities for you if you
distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether
gratis or for a fee, you must give the recipients all the rights that
you have. You must make sure that they, too, receive or can get the
source code. And you must show them these terms so they know their
rights.

We protect your rights with two steps: (1) copyright the software, and
(2) offer you this license which
gives you legal permission to copy,
distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of

Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or

distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to

be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES,

INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR
THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU
General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute

it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this
is what you want to do, use the GNU Lesser General
Public License instead of this License.

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who
decide to use it. You
can use it too, but we suggest you first think carefully about whether

this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library,
whether gratis
or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software
patents pose a constant threat to the existence of
any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use

this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into
another language. (Hereinafter, translation is
included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium,
provided that
you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the
terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be
reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library

with the Library (or with a work based on the Library) on a volume of
a storage or distribution medium does not bring the other work under
the scope of this License.

3. You may opt to apply the terms of the ordinary
GNU General Public
License instead of this License to a given copy of the Library. To do
this, you must alter all the notices that refer to this License, so
that they refer to the ordinary GNU General Public License, version 2,
instead of to this License. (If a newer version than version 2 of the
ordinary GNU General Public License has appeared, then you can specify
that version instead if you wish.) Do not make any other change in
these notices.

Once this change is made in a given copy, it is irreversible for
that copy, so the ordinary GNU General Public License applies to all
subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of
the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or
derivative of it, under Section 2) in object code or executable form
under the terms of Sections 1 and 2 above provided that you accompany
it with the complete corresponding
machine-readable source code, which
must be distributed under the terms of Sections 1 and 2 above on a
medium customarily used for software interchange.

If distribution of object code is made by offering access to copy
from a designated place, then offering equivalent access to copy the
source code from the same place satisfies the requirement to
distribute the source code, even though third parties are not
compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the
Library, but is designed to work with the Library by being compiled or
linked with it, is called a "work that uses the Library". Such a
work, in isolation, is not a derivative work of the Library, and
therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library
creates an executable that is a derivative of the Library (because it
contains portions of the Library), rather than a "work that
uses the
library". The executable is therefore covered by this License.
Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the
object code for the work under the terms of Section 6.
Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany
the work with the complete corresponding
machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate
properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally
distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any
other library
facilities. This must be distributed under the terms of the

Sections above.

b) Give prominent notice with the combined library of the fact
that part of it is a work based on the Library, and explaining
where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if
you do not accept this License. Therefore, by
modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse
you from the conditions of this License. If you cannot
distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply,

and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE,
BE LIABLE TO YOU
FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey
the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public
License along with this library; if not, write to the Free Software
Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301
USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the library, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the
library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!
License

Copyright (C) 2015 Red Hat, Inc.,

This Font Software is licensed under the SIL Open Font License, Version 1.1.
This license is copied below, and is also available with a FAQ at:
http://scripts.sil.org/OFL

SIL OPEN FONT LICENSE
Version 1.1 - 26 February 2007

PREAMBLE
The goals of the Open Font License (OFL) are to stimulate worldwide development
of collaborative font projects, to support the font creation efforts of
academic and linguistic communities, and to provide a free and open framework
in which fonts may be shared and improved in partnership with others.

The OFL allows the licensed fonts to be used, studied, modified and
redistributed freely as long as they are not sold by themselves. The fonts,
including any derivative works, can be bundled, embedded, redistributed and/or
sold with any software provided that any reserved names are not used by

derivative works. The fonts and derivatives, however, cannot be released under any other type of license. The
requirement for fonts to remain under this
license does not apply to any document created using the fonts or their derivatives.

DEFINITIONS
Font Software refers to the set of files released by the Copyright Holder(s) under this license and clearly marked as such. This may include source files, build scripts and documentation.

Reserved Font Name refers to any names specified as such after the copyright statement(s).

Original Version refers to the collection of Font Software components as distributed by the Copyright Holder(s).

Modified Version refers to any derivative made by adding to, deleting, or substitutingin part or in wholeany of the components of the Original Version, by changing formats or by porting the Font Software to a new environment.

Author refers to any designer, engineer, programmer, technical writer or other person who contributed to the Font Software.

PERMISSION & CONDITIONS
Permission is hereby granted, free of charge, to any person obtaining a copy
of
the Font Software, to use, study, copy, merge, embed, modify, redistribute, and sell modified and unmodified copies of the Font Software, subject to the following conditions:

1) Neither the Font Software nor any of its individual components, in Original or Modified Versions, may be sold by itself.

2) Original or Modified Versions of the Font Software may be bundled, redistributed and/or sold with any software, provided that each copy contains the above copyright notice and this license. These can be included either as stand-alone text files, human-readable headers or in the appropriate machine-readable metadata fields within text or binary files as long as those fields can be easily viewed by the user.

3) No Modified Version of the Font Software may use the Reserved Font Name(s) unless explicit written permission is granted by the corresponding Copyright Holder. This restriction only applies to the primary font name as presented to the users.

4) The name(s) of the Copyright Holder(s)

or the Author(s) of the Font Software
shall not be used to promote, endorse or advertise any Modified Version, except
to acknowledge the contribution(s) of the Copyright Holder(s) and the Author(s)
or with their explicit written permission.

5) The Font Software, modified or unmodified, in part or in whole, must be
distributed entirely under this license, and must not be distributed under any
other license. The requirement for fonts to remain under this license does not
apply to any document created using the Font Software.

TERMINATION
This license becomes null and void if any of the above conditions are not met.

DISCLAIMER
THE FONT SOFTWARE IS PROVIDED AS IS, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT,
TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR
ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING
ANY GENERAL, SPECIAL,
INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF
CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE
THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.

1.99 fdisk 2.28.1

1.99.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it. (Some other Free Software Foundation software is covered by
the GNU Lesser General Public License instead.) You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not price.

Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which
gives you legal permission to copy,
distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law:

that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work
are not derived from the Program,
and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution
and only if you
received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to

control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source
code, even though third parties are not
compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing
or modifying
the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For

example, if a patent
license would not permit royalty-free redistribution of the Program by
all those who receive copies directly or indirectly through you, then
the only way you could satisfy both it and this License would be to
refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under
any particular circumstance, the balance of the section is intended to
apply and the section as a whole is intended to apply in other
circumstances.

It is not the purpose of this section to induce you to infringe any
patents or other property right claims or to contest validity of any
such claims; this section has the sole purpose of protecting the
integrity of the free software distribution system, which is
implemented by public license practices. Many people have made
generous contributions to the wide range of software distributed
through that system in reliance on consistent application of that
system; it is up to the author/donor to
decide if he or she is willing
to distribute software through any other system and a licensee cannot
impose that choice.

This section is intended to make thoroughly clear what is believed to
be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in
certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Program under this License
may add an explicit geographical distribution limitation excluding
those countries, so that distribution is permitted only in or among
countries not thus excluded. In such case, this License incorporates
the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions
of the General Public License from time to time. Such new versions will
be similar in spirit to the present version, but may differ in detail to
address new problems or concerns.

Each version is given a distinguishing
version number. If the Program
specifies a version number of this License which applies to it and "any
later version", you have the option of following the terms and conditions
either of that version or of any later version published by the Free
Software Foundation. If the Program does not specify a version number of
this License, you may choose any version ever published by the Free Software
Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU
General Public License as published by
the Free Software Foundation; either version 2 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License along
with this program; if not, write to the Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute
it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this
is what you want to do, use the GNU Lesser General
Public License instead of this License.

This library is free software; you can redistribute it and/or
modify it under the terms of the GNU Lesser General Public
License as published by the Free Software Foundation; either
version 2.1 of the License, or (at your option) any later
version.

The complete text of the license is available in the
../Documentation/licenses/COPYING.LGPLv2.1 file.
WEV @@ WEV[B "1
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
  notice, and the entire permission notice in its entirety,
  including the disclaimer of warranties.
2. Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote
  products derived from this software without specific prior
  written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ALL OF
WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE
LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL
 DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT
OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
USE OF THIS SOFTWARE, EVEN IF NOT ADVISED OF THE POSSIBILITY OF SUCH
DAMAGE.
x   ?"U@,5 @mISmIN<GimCN7g1u|E
43mI,5WEV @@ WEV   @mImImIAmImImI0mImImI*mImI
A0mImImI...
lost+found...

;9GimCN7g

!"#$%&'()*+,-
./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~

!"#$%&'()*+,-
./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~

!"#$%&'()*+,-
./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~

!"#$%&'()*+,-
./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~WEV @@
WEV[B "1
/*
* Copyright (c) 1989 The Regents of the University of California.
* All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the above copyright
*   notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*   notice, this list of conditions and the following disclaimer in the
*   documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*   must display the following acknowledgement:
* This product includes software developed by the University of
* California, Berkeley and its contributors.
* 4. Neither the name of the University nor the names of its contributors
*   may be used to endorse or promote products derived from this software
*
 without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*/
This library is free software; you can redistribute it and/or
modify it under the terms of the Modified BSD License.

The complete text of the license is available in the
../Documentation/licenses/COPYING.BSD-3 file.

1.100 curl 7.30.0

1.100.1 Available under license :

License Mixing
==========

libcurl can be built to use a fair amount of various third party libraries,
libraries that are written and provided by other parties that are distributed
using their own licenses. Even libcurl itself contains code that may cause
problems to some. This document attempts to describe what licenses libcurl and
the other libraries use and what possible dilemmas linking and mixing them all
can lead to for end users.

I am not a lawyer and this is not legal advice!

One common dilemma is that [GPL](https://www.gnu.org/licenses/gpl.html)
licensed code is not allowed to be linked with code licensed under the
[Original BSD license](https://spdx.org/licenses/BSD-4-Clause.html) (with the
announcement clause). You may still build your own copies that use them all,
but distributing them as binaries would be to violate the GPL license - unless
you accompany your license with an
[exception](https://www.gnu.org/licenses/gpl-faq.html#GPLIncompatibleLibs). This
particular problem
 was addressed when the [Modified BSD
license](https://opensource.org/licenses/BSD-3-Clause) was created, which does
not have the announcement clause that collides with GPL.

libcurl

Uses an [MIT style license](https://curl.haxx.se/docs/copyright.html) that is
very liberal.

OpenSSL

(May be used for SSL/TLS support) Uses an Original BSD-style license with an
announcement clause that makes it "incompatible" with GPL. You are not
allowed to ship binaries that link with OpenSSL that includes GPL code
(unless that specific GPL code includes an exception for OpenSSL - a habit
that is growing more and more common). If OpenSSL's licensing is a problem
for you, consider using another TLS library.

GnuTLS

(May be used for SSL/TLS support) Uses the
[LGPL](https://www.gnu.org/licenses/lgpl.html) license. If this is a problem
for you, consider using another TLS library. Also note that GnuTLS itself
depends on and uses other libs (libgcrypt and libgpg-error) and they too

are
LGPL- or GPL-licensed.

WolfSSL

(May be used for SSL/TLS support) Uses the GPL license or a proprietary license. If this is a problem for you, consider using another TLS library.

NSS

(May be used for SSL/TLS support) Is covered by the [MPL](https://www.mozilla.org/MPL/) license, the GPL license and the LGPL license. You may choose to license the code under MPL terms, GPL terms, or LGPL terms. These licenses grant you different permissions and impose different obligations. You should select the license that best meets your needs.

mbedTLS

(May be used for SSL/TLS support) Uses the [Apache 2.0 license](https://opensource.org/licenses/Apache-2.0) or the GPL license. You may choose to license the code under Apache 2.0 terms or GPL terms. These licenses grant you different permissions and impose different obligations. You should select the license that best meets your needs.

BoringSSL

(May be used for SSL/TLS support) As an OpenSSL fork, it has the same license as that.

libressl

(May be used for SSL/TLS support) As an OpenSSL fork, it has the same license as that.

c-ares

(Used for asynchronous name resolves) Uses an MIT license that is very liberal and imposes no restrictions on any other library or part you may link with.

zlib

(Used for compressed Transfer-Encoding support) Uses an MIT-style license that shouldn't collide with any other library.

MIT Kerberos

(May be used for GSS support) MIT licensed, that shouldn't collide with any
other parts.

Heimdal

(May be used for GSS support) Heimdal is Original BSD licensed with the
announcement clause.

GNU GSS

(May be used for GSS support) GNU GSS is GPL licensed. Note that you may not
distribute binary curl packages that uses this if you build curl to also link
and use any Original BSD licensed libraries!

libidn

(Used for IDNA support) Uses the GNU Lesser General Public License [3]. LGPL
is a variation of GPL with slightly less aggressive
"copyleft". This license
requires more requirements to be met when distributing binaries, see the
license for details. Also note that if you distribute a binary that includes
this library, you must also include the full LGPL license text. Please
properly point out what parts of the distributed package that the license
addresses.

OpenLDAP

(Used for LDAP support) Uses a Modified BSD-style license. Since libcurl uses
OpenLDAP as a shared library only, I have not heard of anyone that ships
OpenLDAP linked with libcurl in an app.

libssh2

(Used for scp and sftp support) libssh2 uses a Modified BSD-style license.
COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2019, Daniel Stenberg, <daniel@haxx.se>, and many
contributors, see the THANKS file.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose
with or without fee is hereby granted, provided that the above copyright
notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN

NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not
be used in advertising or otherwise to promote the sale, use or other
dealings
in this Software without prior written authorization of the copyright holder.

1.101 strace 4.13

1.101.1 Available under license :

Copyright (c) 1991, 1992 Paul Kranenburg <pk@cs.few.eur.nl>
Copyright (c) 1993 Branko Lankester <branko@hacktic.nl>
Copyright (c) 1993 Ulrich Pegelow <pegelow@moorea.uni-muenster.de>
Copyright (c) 1995, 1996 Michael Elizabeth Chastain <mec@duracef.shout.net>
Copyright (c) 1993, 1994, 1995, 1996 Rick Sladkey <jrs@world.std.com>
Copyright (C) 1998-2001 Wichert Akkerman <wakkerma@deephackmode.org>
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products
derived from this software
without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
This is the Debian packaged version of strace. For a complete list of
changes from the upstream version please see the changelog.

The upstream sources can be found at http://sourceforge.net/projects/strace/

This is the copyright as found in the upstream sources:

Copyright (c) 1991, 1992 Paul Kranenburg <pk@cs.few.eur.nl>
Copyright (c) 1993 Branko Lankester <branko@hacktic.nl>
Copyright (c) 1993 Ulrich Pegelow <pegelow@moorea.uni-muenster.de>
Copyright (c) 1995, 1996 Michael Elizabeth Chastain <mec@duracef.shout.net>
Copyright (c) 1993, 1994, 1995, 1996 Rick Sladkey <jrs@world.std.com>
Copyright (C) 1998-2003 Wichert Akkerman <wakkerma@deephackmode.org>
Copyright (c) 2002-2008 Roland McGrath <roland@redhat.com>
Copyright (c) 2003-2008 Dmitry V. Levin <ldv@altlinux.org>
Copyright (c) 2007-2008 Jan Kratochvil <jan.kratochvil@redhat.com>
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are
 met:
1. Redistributions of source code must retain the above copyright
  notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products
  derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY
 OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF
THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

1.102 expat 2.2.0

1.102.1 Available under license :

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd
                and Clark Cooper
Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006 Expat maintainers.

Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the

"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be included
in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.
IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE
LIABLE FOR ANY
CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT,
TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,

OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.

1.103 expat 2.1.0

1.103.1 Available under license :

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd
and Clark Cooper
Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006 Expat maintainers.

Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be included
in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.
IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE
LIABLE FOR ANY
CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT,
TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

1.104 rsync 3.1.2

1.104.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for
software and other kinds of works.

The licenses for most software and other practical works are designed
to take away your freedom to share and change the works. By contrast,
the GNU General Public License is intended to guarantee your freedom to
share and change all versions of a program--to make sure it remains free
software for all its users. We, the Free Software Foundation, use the
GNU General Public License for most of our software; it applies also to
any other work released this way by its authors. You can apply it to

your programs, too.

When we speak of free software, we are referring to
freedom, not
price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps:
(1)
assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand
ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could

make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of

copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered
by this License only if the output, given its
content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed;
section 10
makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately
publish on each copy an appropriate copyright notice;
keep intact all notices stating that this License and any
non-permissive terms added in accord with section 7 apply to the code;

keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms

of sections 4 and 5, provided that you also convey the
machine-readable Corresponding Source under the terms of this License,
in one of these ways:

a) Convey the object code in, or embodied in, a physical product
(including a physical distribution medium), accompanied by the
Corresponding Source fixed on a durable physical medium
customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product
(including a physical distribution medium), accompanied by a
written offer, valid for at least three years
and valid for as
long as you offer spare parts or customer support for that product
model, to give anyone who possesses the object code either (1) a
copy of the Corresponding Source for all the software in the
product that is covered by this License, on a durable physical
medium customarily used for software interchange, for a price no
more than your reasonable cost of physically performing this
conveying of source, or (2) access to copy the
Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the
written offer to provide the Corresponding Source. This
alternative is allowed only occasionally and noncommercially, and
only if you received the object code with such an offer, in accord
with subsection 6b.

d) Convey the object code by offering access from a designated
place (gratis or for a charge), and offer equivalent access to the
Corresponding Source in
the same way through the same place at no
further charge. You need not require recipients to copy the
Corresponding Source along with the object code. If the place to
copy the object code is a network server, the Corresponding Source
may be on a different server (operated by you or a third party)
that supports equivalent copying facilities, provided you maintain
clear directions next to the object code saying where to find the
Corresponding Source. Regardless of what server hosts the
Corresponding Source, you remain obligated to ensure that it is
available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided
you inform other peers where the object code and Corresponding
Source of the work are being offered to the general public at no
charge under subsection 6d.

A separable portion of the object code, whose source code is excluded

from the Corresponding Source
as a System Library, need not be
included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any
tangible personal property which is normally used for personal, family,
or household purposes, or (2) anything designed or sold for incorporation
into a dwelling. In determining whether a product is a consumer product,
doubtful cases shall be resolved in favor of coverage. For a particular
product received by a particular user, "normally used" refers to a
typical or common use of that class of product, regardless of the status
of the particular user or of the way in which the particular user
actually uses, or expects or is expected to use, the product. A product
is a consumer product regardless of whether the product has substantial
commercial, industrial or non-consumer uses, unless such uses represent
the only significant mode of use of the product.

"Installation Information" for a User Product means any methods,
procedures, authorization
keys, or other information required to install
and execute modified versions of a covered work in that User Product from
a modified version of its Corresponding Source. The information must
suffice to ensure that the continued functioning of the modified object
code is in no case prevented or interfered with solely because
modification has been made.

If you convey an object code work under this section in, or with, or
specifically for use in, a User Product, and the conveying occurs as
part of a transaction in which the right of possession and use of the
User Product is transferred to the recipient in perpetuity or for a
fixed term (regardless of how the transaction is characterized), the
Corresponding Source conveyed under this section must be accompanied
by the Installation Information. But this requirement does not apply
if neither you nor any third party retains the ability to install
modified object code on the User Product (for example, the work has
been installed in
ROM).

The requirement to provide Installation Information does not include a
requirement to continue to provide support service, warranty, or updates
for a work that has been modified or installed by the recipient, or for
the User Product in which it has been modified or installed. Access to a
network may be denied when the modification itself materially and
adversely affects the operation of the network or violates the rules and
protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided,
in accord with this section must be in a format that is publicly

documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for

any liability that these contractual assumptions directly impose on

those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above
requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright
holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the

licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights
granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or
that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to

address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17.

Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>
This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it

under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what you want to
do, use the GNU Lesser General
Public License instead of this License. But first, please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.
Copyright (c) 1998 Red Hat Software

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
X CONSORTIUM BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN
AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN
CONNECTION WITH THE SOFTWARE OR
THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of the X Consortium shall not be
used in advertising or otherwise to promote the sale, use or other dealings
in this Software without prior written authorization from the X Consortium.

1.105 shadow 4.2.1

1.105.1 Available under license :

NOTE:
This license has been obsoleted by the change to the BSD-style copyright.
You may continue to use this license if you wish, but you are under no
obligation to do so.

(*
This document is freely plagiarised from the 'Artistic Licence',
distributed as part of the Perl v4.0 kit by Larry Wall, which is
available from most major archive sites. I stole it from CrackLib.

Id
*)

This documents purpose is to state the conditions under which this
Package (See definition below) viz: "Shadow", the Shadow Password Suite
which is held by Julianne Frances Haugh, may be copied, such that the
copyright holder maintains some semblance of artistic control over the
development of the package, while giving the users of the package the
right to use and distribute the Package in a more-or-less customary
fashion, plus the right to make reasonable modifications.

So there.

****

Definitions:

A "Package" refers to the collection
of files distributed by the
Copyright Holder, and derivatives of that collection of files created
through textual modification, or segments thereof.

"Standard Version" refers to such a Package if it has not been modified,
or has been modified in accordance with the wishes of the Copyright
Holder.

"Copyright Holder" is whoever is named in the copyright or copyrights
for the package.

"You" is you, if you're thinking about copying or distributing this
Package.

"Reasonable copying fee" is whatever you can justify on the basis of
media cost, duplication charges, time of people involved, and so on.
(You will not be required to justify it to the Copyright Holder, but
only to the computing community at large as a market that must bear the

fee.)

"Freely Available" means that no fee is charged for the item itself, though there may be fees involved in handling the item. It also means that recipients of the item may redistribute it under the same conditions they received it.

1. You may make and give away verbatim copies of the source form of the Standard Version of this Package without restriction, provided that you duplicate all of the original copyright notices and associated disclaimers.

2. You may apply bug fixes, portability fixes and other modifications derived from the Public Domain or from the Copyright Holder. A Package modified in such a way shall still be considered the Standard Version.

3. You may otherwise modify your copy of this Package in any way, provided that you insert a prominent notice in each changed file stating how and when AND WHY you changed that file, and provided that you do at least ONE of the following:

a) place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major archive site such as uunet.uu.net, or by allowing the Copyright Holder to include your modifications in the Standard Version of the Package.

b) use the modified Package only within your corporation or organization.

c) rename any non-standard executables so the names do not conflict with standard executables, which must also be provided, and provide separate documentation for each non-standard executable that clearly documents how it differs from the Standard Version.

d) make other distribution arrangements with the Copyright Holder.

4. You may distribute the programs of this Package in object code or executable form, provided that you do at least ONE of the following:

a) distribute a Standard Version of the executables and library files, together with instructions (in the manual page or equivalent) on where to get the Standard Version.

b) accompany the distribution with the machine-readable source of the Package with your modifications.

c) accompany any non-standard executables with their corresponding
Standard Version executables, giving the non-standard executables
non-standard names, and clearly
documenting the differences in manual
pages (or equivalent), together with instructions on where to get the
Standard Version.

d) make other distribution arrangements with the Copyright Holder.

5. You may charge a reasonable copying fee for any distribution of this
Package. You may charge any fee you choose for support of this Package.
YOU MAY NOT CHARGE A FEE FOR THIS PACKAGE ITSELF. However, you may
distribute this Package in aggregate with other (possibly commercial)
programs as part of a larger (possibly commercial) software distribution
provided that YOU DO NOT ADVERTISE this package as a product of your
own.

6. The name of the Copyright Holder may not be used to endorse or
promote products derived from this software without specific prior
written permission.

7. THIS PACKAGE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF
MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The End
GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
675 Mass Ave, Cambridge, MA 02139, USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it. (Some other Free Software Foundation software is covered by
the GNU Library General Public License instead.) You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not

price. Our General Public Licenses are designed
to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid
anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate to certain responsibilities for you if you
distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether
gratis or for a fee, you must give the recipients all the rights that
you have. You must make sure that they, too, receive or can get the
source code. And you must show them these terms so they know their
rights.

We protect your rights with two steps: (1) copyright the software, and
(2) offer you this license which gives you legal permission to copy,
distribute
and/or modify the software.

Also, for each author's protection and ours, we want to make certain
that everyone understands that there is no warranty for this free
software. If the software is modified by someone else and passed on, we
want its recipients to know that what they have is not the original, so
that any problems introduced by others will not reflect on the original
authors' reputations.

Finally, any free program is threatened constantly by software
patents. We wish to avoid the danger that redistributors of a free
program will individually obtain patent licenses, in effect making the
program proprietary. To prevent this, we have made it clear that any
patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and
modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work
which contains
a notice placed by the copyright holder saying it may be distributed
under the terms of this General Public License. The "Program", below,
refers to any such program or work, and a "work based on the Program"
means either the Program or any derivative work under copyright law:

that is to say, a work containing the Program or a portion of it,
either verbatim or with modifications and/or translated into another
language. (Hereinafter, translation is included without limitation in
the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not
covered by this License; they are outside its scope. The act of
running the Program is not restricted, and the output from the Program
is covered only if its contents constitute a work based on the
Program (independent of having been made by running the Program).
Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim
copies of the Program's
source code as you receive it, in any medium, provided that you
conspicuously and appropriately publish on each copy an appropriate
copyright notice and disclaimer of warranty; keep intact all the
notices that refer to this License and to the absence of any warranty;
and give any other recipients of the Program a copy of this License
along with the Program.

You may charge a fee for the physical act of transferring a copy, and
you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion
of it, thus forming a work based on the Program, and copy and
distribute such modifications or work under the terms of Section 1
above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices
stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in
whole
or in part contains or is derived from the Program or any
part thereof, to be licensed as a whole at no charge to all third
parties under the terms of this License.

c) If the modified program normally reads commands interactively
when run, you must cause it, when started running for such
interactive use in the most ordinary way, to print or display an
announcement including an appropriate copyright notice and a
notice that there is no warranty (or else, saying that you provide
a warranty) and that users may redistribute the program under
these conditions, and telling the user how to view a copy of this
License. (Exception: if the Program itself is interactive but
does not normally print such an announcement, your work based on
the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably
considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it,
under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code
or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any

associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy
the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6.
Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you

may not distribute the Program at all. For example, if a patent
license would not permit royalty-free
redistribution of the Program by
all those who receive copies directly or indirectly through you, then
the only way you could satisfy both it and this License would be to
refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under
any particular circumstance, the balance of the section is intended to
apply and the section as a whole is intended to apply in other
circumstances.

It is not the purpose of this section to induce you to infringe any
patents or other property right claims or to contest validity of any
such claims; this section has the sole purpose of protecting the
integrity of the free software distribution system, which is
implemented by public license practices. Many people have made
generous contributions to the wide range of software distributed
through that system in reliance on consistent application of that
system; it is up to the author/donor to decide if he or she is willing
to distribute software through
any other system and a licensee cannot
impose that choice.

This section is intended to make thoroughly clear what is believed to
be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in
certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Program under this License
may add an explicit geographical distribution limitation excluding
those countries, so that distribution is permitted only in or among
countries not thus excluded. In such case, this License incorporates
the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions
of the General Public License from time to time. Such new versions will
be similar in spirit to the present version, but may differ in detail to
address new problems or concerns.

Each version is given a distinguishing version number. If the Program
specifies a version number
of this License which applies to it and "any
later version", you have the option of following the terms and conditions
either of that version or of any later version published by the Free
Software Foundation. If the Program does not specify a version number of
this License, you may choose any version ever published by the Free Software
Foundation.

10. If you wish to incorporate parts of the Program into other free
programs whose distribution conditions are different, write to the author
to ask for permission. For software which is copyrighted by the Free
Software Foundation, write to the Free Software Foundation; we sometimes
make exceptions for this. Our decision will be guided by the two goals
of preserving the free status of all derivatives of our free software and
of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY
FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE
LAW. EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES
PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED
OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS
TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE
PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING,
REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING
WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR
REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES,
INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING
OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED
TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY
YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER
PROGRAMS),
EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE
POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

1.106 perl 5.20.0

1.106.1 Available under license :

The "Artistic License"

Preamble

The intent of this document is to state the conditions under which a

Package may be copied, such that the Copyright Holder maintains some
semblance of artistic control over the development of the package,
while giving the users of the package the right to use and distribute
the Package in a more-or-less customary fashion, plus the right to make
reasonable modifications.

Definitions:

"Package" refers to the collection of files distributed by the
Copyright Holder, and derivatives of that collection of files
created through textual modification.

"Standard Version" refers to such a Package if it has not been
modified, or has been modified in accordance with the wishes
of the Copyright Holder as specified below.

"Copyright Holder" is whoever is named in the copyright or
copyrights for the package.

"You" is you, if you're thinking
about copying or distributing
this Package.

"Reasonable copying fee" is whatever you can justify on the
basis of media cost, duplication charges, time of people involved,
and so on. (You will not be required to justify it to the
Copyright Holder, but only to the computing community at large
as a market that must bear the fee.)

"Freely Available" means that no fee is charged for the item
itself, though there may be fees involved in handling the item.
It also means that recipients of the item may redistribute it
under the same conditions they received it.

1. You may make and give away verbatim copies of the source form of the
Standard Version of this Package without restriction, provided that you
duplicate all of the original copyright notices and associated disclaimers.

2. You may apply bug fixes, portability fixes and other modifications
derived from the Public Domain or from the Copyright Holder.
A Package
modified in such a way shall still be considered the Standard Version.

3. You may otherwise modify your copy of this Package in any way, provided
that you insert a prominent notice in each changed file stating how and
when you changed that file, and provided that you do at least ONE of the
following:

a) place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major archive site such as uunet.uu.net, or by allowing the Copyright Holder to include your modifications in the Standard Version of the Package.

b) use the modified Package only within your corporation or organization.

c) rename any non-standard executables so the names do not conflict with standard executables, which must also be provided, and provide a separate manual page for each non-standard executable that clearly documents how it
differs from the Standard Version.

d) make other distribution arrangements with the Copyright Holder.

4. You may distribute the programs of this Package in object code or executable form, provided that you do at least ONE of the following:

a) distribute a Standard Version of the executables and library files, together with instructions (in the manual page or equivalent) on where to get the Standard Version.

b) accompany the distribution with the machine-readable source of the Package with your modifications.

c) give non-standard executables non-standard names, and clearly document the differences in manual pages (or equivalent), together with instructions on where to get the Standard Version.

d) make other distribution arrangements with the Copyright Holder.

5. You may charge a reasonable copying fee for any distribution of this Package. You may charge any fee you choose for support of this Package. You may not charge a fee for this Package
itself. However,
you may distribute this Package in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution provided that you do not advertise this Package as a product of your own. You may embed this Package's interpreter within an executable of yours (by linking); this shall be construed as a mere form of aggregation, provided that the complete Standard Version of the interpreter is so embedded.

6. The scripts and library files supplied as input to or produced as output from the programs of this Package do not automatically fall under the copyright of this Package, but belong to whoever generated them, and may be sold commercially, and may be aggregated with this

Package. If such scripts or library files are aggregated with this
Package via the so-called "undump" or "unexec" methods of producing a
binary executable image, then distribution of such an image shall
neither be construed as a distribution of this Package
 nor shall it
fall under the restrictions of Paragraphs 3 and 4, provided that you do
not represent such an executable image as a Standard Version of this
Package.

7. C subroutines (or comparably compiled subroutines in other
languages) supplied by you and linked into this Package in order to
emulate subroutines and variables of the language defined by this
Package shall not be considered part of this Package, but are the
equivalent of input as in Paragraph 6, provided these subroutines do
not change the language in any way that would cause it to fail the
regression tests for the language.

8. Aggregation of this Package with a commercial distribution is always
permitted provided that the use of this Package is embedded; that is,
when no overt attempt is made to make this Package's interfaces visible
to the end user of the commercial distribution. Such use shall not be
construed as a distribution of this Package.

9. The name of the Copyright Holder may not be used to endorse or promote
products
 derived from this software without specific prior written permission.

10. THIS PACKAGE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The End

---
abstract: 'Build and install Perl modules'
author:
 - 'Ken Williams <kwilliams@cpan.org>'
 - "Development questions, bug reports, and patches should be sent to the\nModule-Build mailing list at <module-build@perl.org>."
build_requires:
 File::Temp: 0.15
 Test::Harness: 3.16
 Test::More: 0.49
generated_by: 'Module::Build version 0.3608'
license: gpl
meta-spec:
 url: http://module-build.sourceforge.net/META-spec-v1.4.html
 version: 1.4
name: Module-Build

resources:
 MailingList: mailto:module-build@perl.org
 license: http://dev.perl.org/licenses/
 repository: http://github.com/dagolden/module-build/
version: 3

This program, "bzip2", the associated library "libbzip2", and all
documentation, are copyright (C) 1996-2010 Julian R Seward. All
rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

1. Redistributions of source code must retain the above copyright
  notice, this list of conditions and the following disclaimer.

2. The origin of this software must not be misrepresented; you must
  not claim that you wrote the original software. If you use this
  software in a product, an acknowledgment in the product
  documentation would be appreciated but is not required.

3. Altered source versions must be plainly marked as such, and must
  not be misrepresented as being the original software.

4. The name of the author may not be used to endorse or promote
  products derived from this software without specific
 prior written
  permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS
OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY
DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE
GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Julian Seward, jseward@bzip.org
bzip2/libbzip2 version 1.0.6 of 6 September 2010

GNU GENERAL PUBLIC LICENSE
Version 1, February 1989

Copyright (C) 1989 Free Software Foundation, Inc.
51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The license agreements of most software companies try to keep users at the mercy of those companies. By contrast, our General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. The General Public License applies to the Free Software Foundation's software and to any other program whose authors commit to using it. You can use it for your programs, too.

When we speak of free software, we are referring to freedom, not price. Specifically, the General Public License is designed to make sure that you have the freedom to
give away or sell copies of free
software, that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of a such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must tell them their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that
everyone understands that there is no warranty for this free
software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original

authors' reputations.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any work containing the Program or a portion of it, either verbatim or with modifications. Each licensee is addressed as "you".

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this General Public License and to the absence of any warranty; and give any other recipients of the Program a copy of this General Public License along with the Program. You may charge a fee for the physical act of transferring a copy.

2. You may modify your copy or copies of the Program or any portion of it, and copy and distribute such modifications under the terms of Paragraph 1 above, provided that you also do the following:

a) cause the modified files to carry prominent notices stating that you changed the files and the date of any change; and

b) cause the whole of any work that you distribute or publish, that in whole or in part contains the Program or any part thereof, either with or without modifications, to be licensed at no charge to all third parties under the terms of this General Public License (except that you may choose to grant warranty protection to some or all third parties, at your option).

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the simplest and most usual way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this General

Public License.

d) You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

Mere aggregation of another independent work with the Program (or its derivative) on a volume of a storage or distribution medium does not bring the other work under the scope of these terms.

3. You may copy and distribute the Program (or a portion or derivative of it, under Paragraph 2) in object code or executable form under the terms of Paragraphs 1 and 2 above provided that you also do one of the following:

a) accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Paragraphs 1 and 2 above; or,

b) accompany it with a written offer, valid for at least three years, to give any third party free (except for a nominal charge for the cost of distribution) a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Paragraphs 1 and 2 above; or,

c) accompany it with the information you received as to where the corresponding source code may be obtained. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form alone.)

Source code for a work means the preferred form of the work for making modifications to it. For an executable file, complete source code means all the source code for all modules it contains; but, as a special exception, it need not include source code for modules which are standard libraries that accompany the operating system on which the executable file runs, or for standard header files or definitions files that accompany that operating system.

4. You may not copy, modify, sublicense, distribute or transfer the Program except as expressly provided under this General Public License. Any attempt otherwise to copy, modify, sublicense, distribute or transfer the Program is void, and will automatically terminate your rights to use the Program under this License. However, parties who have received copies, or rights to use copies, from you under this General Public License will not have their licenses terminated so long as such parties remain

in full compliance.

5. By copying, distributing or modifying the Program (or any work based on the Program) you indicate your acceptance of this license to do so, and all its terms and conditions.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein.

7. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of the license which applies to it and "any later version", you have the option of following the terms and conditions
either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the license, you may choose any version ever published by the Free Software Foundation.

8. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

9. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE
THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

10. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING

WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Appendix: How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to humanity, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) 19yy <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 1, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19xx name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the
appropriate parts of the General Public License.
Of course, the
commands you use may be called something other than `show w' and `show
c'; they could even be mouse-clicks or menu items--whatever suits your
program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the
program `Gnomovision' (a program to direct compilers to make passes
at assemblers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

That's all there is to it!
This software is copyright (c) 2017 by Ken Williams.

This is free software; you can redistribute it and/or modify it under
the same terms as the Perl 5 programming language system itself.

Terms of the Perl programming language system itself

a) the GNU General Public License as published by the Free
Software Foundation; either version 1, or (at your option) any
later version, or
b) the "Artistic License"

--- The GNU General Public License, Version 1, February 1989 ---

This software is Copyright (c) 2017 by Ken Williams.

This is free software, licensed under:

The GNU General Public License, Version 1, February 1989

GNU GENERAL PUBLIC LICENSE
Version 1, February 1989

Copyright (C) 1989 Free Software Foundation, Inc.
51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The license agreements of most software companies try to keep users at the mercy of those companies. By contrast, our General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. The General Public License applies to the Free Software Foundation's software and to any other program whose authors commit to using it. You can use it for your programs, too.

When we speak of free software, we are referring to freedom, not price. Specifically, the General Public License is designed to make sure that you have the freedom to give away or sell copies of free software, that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate
to certain responsibilities for you if you
distribute copies of the software, or if you modify it.

For example, if you distribute copies of a such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must tell them their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

The precise terms and conditions for copying, distribution and modification
follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any work containing the Program or a portion of it, either verbatim or with modifications. Each licensee is addressed as "you".

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this General Public License and to the absence of any warranty; and give any other recipients of the Program a copy of this General Public License along
with the Program. You may charge a fee for the physical act of transferring a copy.

2. You may modify your copy or copies of the Program or any portion of it, and copy and distribute such modifications under the terms of Paragraph 1 above, provided that you also do the following:

a) cause the modified files to carry prominent notices stating that you changed the files and the date of any change; and

b) cause the whole of any work that you distribute or publish, that in whole or in part contains the Program or any part thereof, either with or without modifications, to be licensed at no charge to all third parties under the terms of this General Public License (except that you may choose to grant warranty protection to some or all third parties, at your option).

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the simplest and most
usual way, to print or display an
announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this General Public License.

d) You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

Mere aggregation of another independent work with the Program (or its derivative) on a volume of a storage or distribution medium does not bring the other work under the scope of these terms.

3. You may copy and distribute the Program (or a portion or derivative of it, under Paragraph 2) in object code or executable form under the terms of Paragraphs 1 and 2 above provided that you also do one of the following:

a) accompany it with the complete corresponding machine-readable source code, which
must be distributed under the terms of
Paragraphs 1 and 2 above; or,

b) accompany it with a written offer, valid for at least three years, to give any third party free (except for a nominal charge for the cost of distribution) a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Paragraphs 1 and 2 above; or,

c) accompany it with the information you received as to where the corresponding source code may be obtained. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form alone.)

Source code for a work means the preferred form of the work for making modifications to it. For an executable file, complete source code means all the source code for all modules it contains; but, as a special exception, it need not include source code for modules which are standard libraries that accompany the operating system on which
the executable
file runs, or for standard header files or definitions files that accompany that operating system.

4. You may not copy, modify, sublicense, distribute or transfer the Program except as expressly provided under this General Public License. Any attempt otherwise to copy, modify, sublicense, distribute or transfer the Program is void, and will automatically terminate your rights to use the Program under this License. However, parties who have received copies, or rights to use copies, from you under this General Public License will not have their licenses terminated so long as such parties remain in full compliance.

5. By copying, distributing or modifying the Program (or any work based on the Program) you indicate your acceptance of this license to do so, and all its terms and conditions.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original

licensor to copy, distribute or modify
the Program subject to these
terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein.

7. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of the license which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the license, you may choose any version ever published by the Free Software Foundation.

8. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the
author
to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

9. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

10. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Appendix: How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to humanity, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) 19yy <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 1, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19xx name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show

c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here a sample; alter the names:

Yoyodyne, Inc., hereby disclaims
all copyright interest in the
program `Gnomovision' (a program to direct compilers to make passes
at assemblers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

That's all there is to it!

--- The Artistic License 1.0 ---

This software is Copyright (c) 2017 by Ken Williams.

This is free software, licensed under:

The Artistic License 1.0

The Artistic License

Preamble

The intent of this document is to state the conditions under which a Package may be copied, such that the Copyright Holder maintains some semblance of artistic control over the development of the package, while giving the users of the package the right to use and distribute the Package in a more-or-less customary fashion, plus the right to make reasonable modifications.

Definitions:

- "Package" refers to the collection of files distributed by the Copyright Holder, and derivatives of that collection of files created through textual modification.

- "Standard Version" refers to such a Package if it has not been modified, or has been modified in accordance with the wishes of the Copyright Holder.
- "Copyright Holder" is whoever is named in the copyright or copyrights for the package.
- "You" is you, if you're thinking about copying or distributing this Package.

- "Reasonable copying fee" is whatever you can justify on the basis of media cost, duplication charges, time of people involved, and so on. (You will not be required to justify it to the Copyright Holder, but only to the computing community at large as a market that must bear the fee.)
- "Freely Available" means that no fee is charged for the item itself, though there may be fees involved in handling the item. It also means that recipients of the item may redistribute it under the same conditions they received it.

1. You may make and give away verbatim copies of the source form of the Standard Version of this Package without
restriction, provided that you
duplicate all of the original copyright notices and associated disclaimers.

2. You may apply bug fixes, portability fixes and other modifications derived from the Public Domain or from the Copyright Holder. A Package modified in such a way shall still be considered the Standard Version.

3. You may otherwise modify your copy of this Package in any way, provided that you insert a prominent notice in each changed file stating how and when you changed that file, and provided that you do at least ONE of the following:

a) place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major archive site such as ftp.uu.net, or by allowing the Copyright Holder to include your modifications in the Standard Version of the Package.

b) use the modified Package only within your corporation or organization.

c)
rename any non-standard executables so the names do not conflict with standard executables, which must also be provided, and provide a separate manual page for each non-standard executable that clearly documents how it differs from the Standard Version.

d) make other distribution arrangements with the Copyright Holder.

4. You may distribute the programs of this Package in object code or executable form, provided that you do at least ONE of the following:

a) distribute a Standard Version of the executables and library files, together with instructions (in the manual page or equivalent) on where to get the Standard Version.

b) accompany the distribution with the machine-readable source of the Package with your modifications.

c) accompany any non-standard executables with their corresponding Standard Version executables, giving the non-standard executables non-standard names, and clearly documenting the differences in manual pages (or equivalent), together with instructions on where to get the Standard Version.

d) make other distribution arrangements with the Copyright Holder.

5. You may charge a reasonable copying fee for any distribution of this Package. You may charge any fee you choose for support of this Package. You may not charge a fee for this Package itself. However, you may distribute this Package in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution provided that you do not advertise this Package as a product of your own.

6. The scripts and library files supplied as input to or produced as output from the programs of this Package do not automatically fall under the copyright of this Package, but belong to whomever generated them, and may be sold commercially, and may be aggregated with this Package.

7. C or perl subroutines supplied by you and linked into this Package shall not be considered part of this Package.

8. The name of the Copyright Holder may not be used to endorse or promote products derived from this software without specific prior written permission.

9. THIS PACKAGE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The End
#!perl

=head1 NAME

copyright.t

=head1 DESCRIPTION

Tests that the latest copyright years in the top-level README file and the C<perl -v> output match each other.

If the test fails, update at least one of README and perl.c so that they match reality.

Optionally you can pass the C<--now> option to check they are at the current year. This isn't checked by default, so that it doesn't fail for people

working on older releases. It should be run before making a new release.

=cut

```
use strict;
use Config;
BEGIN { require './test.pl' }

if ( $Config{usecrosscompile} ) {
 skip_all( "Not all files are available during cross-compilation" );
}

my ($opt) = @ARGV;

my $readme_year = readme_year();
my $v_year = v_year();

# Check that both copyright dates are up-to-date, but only if requested, so
# that tests still pass for people intentionally working on older versions:
if ($opt eq '--now')
{
 my $current_year = (gmtime)[5] + 1900;
 is $v_year, $current_year, 'perl -v copyright includes current
 year';
 is $readme_year, $current_year, 'README copyright includes current year';
}

# Otherwise simply check that the two copyright dates match each other:
else
{
 is $readme_year, $v_year, 'README and perl -v copyright dates match';
}

done_testing;


sub readme_year
# returns the latest copyright year from the top-level README file
{

 open my $readme, '<', '../README' or die "Opening README failed: $!";

 # The copyright message is the first paragraph:
 local $/ = '';
 my $copyright_msg = <$readme>;

 my ($year) = $copyright_msg =~ /.*\b(\d{4,})/s
    or die "Year not found in README copyright message '$copyright_msg'";
```

```
 $year;
}


sub v_year
# returns the latest copyright year shown in perl -v
{

 my $output = runperl switches => ['-v'];
 my ($year) = $output =~ /copyright 1987.*\b(\d{4,})/i
    or die "Copyright statement not found in perl -v output '$output'";

 $year;
}
```

1.107 dnsmasq 2.76

1.107.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it. (Some other Free Software Foundation software is covered by
the GNU Library General Public License instead.) You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price. Our General Public Licenses
are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of

running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you

distribute the same sections as part of a whole which is a work based
on the Program, the distribution of the whole must be on the terms of
this License, whose permissions for other licensees extend to the
entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest
your rights to work written entirely by you; rather, the intent is to
exercise the right to control the distribution of derivative or
collective works based on the Program.

In addition, mere aggregation of another work not based on the Program
with the Program (or with a work based on the Program) on a volume of
a storage or distribution medium does not bring the other work under
the scope of this License.

3. You may copy and distribute the Program
(or a work based on it,
under Section 2) in object code or executable form under the terms of
Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable
source code, which must be distributed under the terms of Sections
1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three
years, to give any third party, for a charge no more than your
cost of physically performing source distribution, a complete
machine-readable copy of the corresponding source code, to be
distributed under the terms of Sections 1 and 2 above on a medium
customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer
to distribute corresponding source code. (This alternative is
allowed only for noncommercial distribution and only if you
received the program
in object code or executable form with such
an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for
making modifications to it. For an executable work, complete source
code means all the source code for all modules it contains, plus any
associated interface definition files, plus the scripts used to
control compilation and installation of the executable. However, as a
special exception, the source code distributed need not include
anything that is normally distributed (in either source or binary
form) with the major components (compiler, kernel, and so on) of the
operating system on which the executable runs, unless that component
itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled
to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based
on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit
royalty-free redistribution of the Program by
all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute
software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies
a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and

of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED
BY APPLICABLE LAW. EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS),
EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) 19yy <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version
2 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19yy name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands
`show w' and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this is what you want to do, use the GNU Library General
Public License instead of this License.

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic

pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand
ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees"
and
"recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other

parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those

subprograms and other parts of the work.

The Corresponding Source need not include anything that users
can regenerate automatically from other parts of the Corresponding
Source.

The Corresponding Source for a work in source code form is that
same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of
copyright on the Program, and are irrevocable provided the stated
conditions are met. This License explicitly affirms your unlimited
permission to run the unmodified Program. The output from running a
covered work is covered
by this License only if the output, given its
content, constitutes a covered work. This License acknowledges your
rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not
convey, without conditions so long as your license otherwise remains
in force. You may convey covered works to others for the sole purpose
of having them make modifications exclusively for you, or provide you
with facilities for running those works, provided that you comply with
the terms of this License in conveying all material for which you do
not control copyright. Those thus making or running the covered works
for you must do so exclusively on your behalf, under your direction
and control, on terms that prohibit them from making any copies of
your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under
the conditions stated below. Sublicensing is not allowed;
section 10
makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological
measure under any applicable law fulfilling obligations under article
11 of the WIPO copyright treaty adopted on 20 December 1996, or
similar laws prohibiting or restricting circumvention of such
measures.

When you convey a covered work, you waive any legal power to forbid
circumvention of technological measures to the extent such circumvention
is effected by exercising rights under this License with respect to
the covered work, and you disclaim any intention to limit operation or

modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately
publish on each copy an appropriate copyright notice;
keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to
"keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work,

and which are not combined with it such as to form a larger program,
in or on a volume of a storage or distribution
medium, is called an
"aggregate" if the compilation and its resulting copyright are not
used to limit the access or legal rights of the compilation's users
beyond what the individual works permit. Inclusion of a covered work
in an aggregate does not cause this License to apply to the other
parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms
of sections 4 and 5, provided that you also convey the
machine-readable Corresponding Source under the terms of this License,
in one of these ways:

a) Convey the object code in, or embodied in, a physical product
(including a physical distribution medium), accompanied by the
Corresponding Source fixed on a durable physical medium
customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product
(including a physical distribution medium), accompanied by a
written offer, valid for at least three years
and valid for as
long as you offer spare parts or customer support for that product
model, to give anyone who possesses the object code either (1) a
copy of the Corresponding Source for all the software in the
product that is covered by this License, on a durable physical
medium customarily used for software interchange, for a price no
more than your reasonable cost of physically performing this
conveying of source, or (2) access to copy the
Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the
written offer to provide the Corresponding Source. This
alternative is allowed only occasionally and noncommercially, and
only if you received the object code with such an offer, in accord
with subsection 6b.

d) Convey the object code by offering access from a designated
place (gratis or for a charge), and offer equivalent access to the
Corresponding Source in
the same way through the same place at no
further charge. You need not require recipients to copy the
Corresponding Source along with the object code. If the place to
copy the object code is a network server, the Corresponding Source
may be on a different server (operated by you or a third party)

that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in

ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or

requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on

those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above
requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright

holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright
holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights

granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work

in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed

under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17.
Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License

along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>
This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what you want to
do, use the GNU Lesser General
Public License instead of this License. But first, please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.

1.108 expat 2.1.1

1.108.1 Available under license :

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd
and Clark Cooper
Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006 Expat maintainers.

Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be included
in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.
IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE
LIABLE FOR ANY
CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT,
TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,

OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

1.109 log-rotate 3.9.1

1.109.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
675 Mass Ave, Cambridge, MA 02139, USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed
to make sure that you
have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute
and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third

parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium

customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6.
Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to

these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions

of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number
of this License which applies to it and "any
later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE
LAW. EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS),
EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest
possible use to the public, the best way to achieve this is to make it
free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest
to attach them to the start of each source file to most effectively
convey the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) 19yy <name of author>

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation; either version 2 of the License,
or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19yy name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should
show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.
Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation`s software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the
freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for

each author`s protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors` reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone`s free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under
the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program`s source code as you receive it, in any medium, provided that you conspicuously
and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge
to all third parties under the terms of this License.
c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this

License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)
These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works.
But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it
with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)
The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all
the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program
is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you

permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not
impose any further restrictions on the recipients` exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this
section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in
certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version
number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are

different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the program`s name and an idea of what it does.
Copyright (C) yyyy name of author

This program is free software; you can redistribute it and/or
modify it under the terms of the GNU General Public License
as published by the Free Software Foundation; either version 2
of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the

GNU General Public License for more details.

You should have received a copy of the
GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.
Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details
type `show w`. This is free software, and you are welcome
to redistribute it under certain conditions; type `show c`
for details.
The hypothetical commands `show w` and `show c` should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w` and `show c`; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer"
for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright
interest in the program `Gnomovision`
(which makes passes at compilers) written
by James Hacker.

signature of Ty Coon, 1 April 1989
Ty Coon, President of Vice
This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

1.110 libksba 1.3.4

1.110.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for
software and other kinds of works.

The licenses for most software and other practical works are designed
to take away your freedom to share and change the works. By contrast,
the GNU General Public License is intended to guarantee your freedom to
share and change all versions of a program--to make sure it remains free
software for all its users. We, the Free Software Foundation, use the
GNU General Public License for most of our software; it applies also to
any other work released this way by its authors. You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price. Our General Public Licenses
are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
them if you wish), that you receive source code or can get it if you
want it, that you can change the software or use pieces of it in new
free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you
these rights or asking you to surrender the rights. Therefore, you have
certain responsibilities if you distribute copies of the software, or if
you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether
gratis or for a fee, you must pass on to the recipients the same
freedoms that you received. You must make sure that they, too, receive
or can get the source code. And you must show them these terms so they
know their rights.

Developers that use the GNU GPL protect your rights with two steps:
(1) assert copyright on the software, and (2) offer
you this License
giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains
that there is no warranty for this free software. For both users' and
authors' sake, the GPL requires that modified versions be marked as
changed, so that their problems will not be attributed erroneously to
authors of previous versions.

Some devices are designed to deny users access to install or run
modified versions of the software inside them, although the manufacturer
can do so. This is fundamentally incompatible with the aim of
protecting users' freedom to change the software. The systematic
pattern of such abuse occurs in the area of products for individuals to
use, which is precisely where it is most unacceptable. Therefore, we

have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate
Legal Notices"
to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than
the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing
those activities but
which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content,
constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal
Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of

technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep
intact all notices stating that this License and any
non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license
the entire work, as a whole, under this
License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an

"aggregate" if the compilation and
its resulting copyright are not
used to limit the access or legal rights of the compilation's users
beyond what the individual works permit. Inclusion of a covered work
in an aggregate does not cause this License to apply to the other
parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms
of sections 4 and 5, provided that you also convey the
machine-readable Corresponding Source under the terms of this License,
in one of these ways:

a) Convey the object code in, or embodied in, a physical product
(including a physical distribution medium), accompanied by the
Corresponding Source fixed on a durable physical medium
customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product
(including a physical distribution medium), accompanied by a
written offer, valid for at least three years and valid for as
long as you offer spare parts or customer
support for that product
model, to give anyone who possesses the object code either (1) a
copy of the Corresponding Source for all the software in the
product that is covered by this License, on a durable physical
medium customarily used for software interchange, for a price no
more than your reasonable cost of physically performing this
conveying of source, or (2) access to copy the
Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the
written offer to provide the Corresponding Source. This
alternative is allowed only occasionally and noncommercially, and
only if you received the object code with such an offer, in accord
with subsection 6b.

d) Convey the object code by offering access from a designated
place (gratis or for a charge), and offer equivalent access to the
Corresponding Source in the same way through the same place at no
further charge.
You need not require recipients to copy the
Corresponding Source along with the object code. If the place to
copy the object code is a network server, the Corresponding Source
may be on a different server (operated by you or a third party)
that supports equivalent copying facilities, provided you maintain
clear directions next to the object code saying where to find the

Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object
code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute
modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information

does not include a
requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in
this License, to the extent
that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections
15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your
receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time
you convey a covered work, the recipient automatically
receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not

impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that

country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed

under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING
WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS
THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY
GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE
USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF
DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD
PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS),
EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF
SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of
warranty and limitation of liability provided
above cannot be given local legal effect according to their terms,
reviewing courts shall apply local law that most closely approximates
an absolute waiver of all civil liability in connection with the
Program, unless a warranty or assumption of liability accompanies a
copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest
possible use to the public, the best way to achieve this is to make it
free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest
to attach them to the start of each source file to most effectively
state the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea
of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation, either version 3 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License

along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>
This program comes with ABSOLUTELY
NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what you want to do, use the GNU Lesser General
Public License instead of this License. But first,
please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.
GNU LESSER GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates
the terms and conditions of version 3 of the GNU General Public
License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, "this License" refers to version 3 of the GNU Lesser
General Public License, and the "GNU GPL" refers to version 3 of the GNU
General Public License.

"The Library" refers to a covered work governed by this License,

other than an Application or a Combined Work as defined below.

An "Application" is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object

code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version

of the Library that is interface-compatible
with the Linked
Version.

e) Provide Installation Information, but only if you would otherwise
be required to provide such information under section 6 of the
GNU GPL, and only to the extent that such information is
necessary to install and execute a modified version of the
Combined Work produced by recombining or relinking the
Application with a modified version of the Linked Version. (If
you use option 4d0, the Installation Information must accompany
the Minimal Corresponding Source and Corresponding Application
Code. If you use option 4d1, you must provide the Installation
Information in the manner specified by section 6 of the GNU GPL
for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the
Library side by side in a single library together with other library
facilities that are not Applications and are not covered by this
License, and convey such a combined
library under terms of your
choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based
on the Library, uncombined with any other library facilities,
conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it
is a work based on the Library, and explaining where to find the
accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions
of the GNU Lesser General Public License from time to time. Such new
versions will be similar in spirit to the present version, but may
differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the
Library as you received it specifies that a certain numbered version
of the GNU Lesser General Public License "or any later version"
applies to it, you have the option
of following the terms and
conditions either of that published version or of any later version
published by the Free Software Foundation. If the Library as you
received it does not specify a version number of the GNU Lesser

General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price.

Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and

(2) offer you this license which
gives you legal permission to copy,
distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain
that everyone understands that there is no warranty for this free
software. If the software is modified by someone else and passed on, we
want its recipients to know that what they have is not the original, so
that any problems introduced by others will not reflect on the original
authors' reputations.

Finally, any free program is threatened constantly by software
patents. We wish to avoid the danger that redistributors of a free
program will individually obtain patent licenses, in effect making the
program proprietary. To prevent this, we have made it clear that any
patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and
modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains
a notice placed by the copyright holder saying it may be distributed
under the terms of this General Public License. The "Program", below,
refers to any such program or work, and a "work based on the Program"
means either the Program or any derivative work under copyright law:
that is to say, a work containing the Program or a portion of it,
either verbatim or with modifications and/or translated into another
language. (Hereinafter, translation is included without limitation in
the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not
covered by this License; they are outside its scope. The act of
running the Program is not restricted, and the output from the Program
is covered only if its contents constitute a work based on the
Program (independent of having been made by running the Program).
Whether that is true depends on what the
Program does.

1. You may copy and distribute verbatim copies of the Program's
source code as you receive it, in any medium, provided that you
conspicuously and appropriately publish on each copy an appropriate
copyright notice and disclaimer of warranty; keep intact all the
notices that refer to this License and to the absence of any warranty;
and give any other recipients of the Program a copy of this License
along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under

the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such

parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to

decide if he or she is willing
to distribute software through any other system and a licensee cannot
impose that choice.

This section is intended to make thoroughly clear what is believed to
be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in
certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Program under this License
may add an explicit geographical distribution limitation excluding
those countries, so that distribution is permitted only in or among
countries not thus excluded. In such case, this License incorporates
the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions
of the General Public License from time to time. Such new versions will
be similar in spirit to the present version, but may differ in detail to
address new problems or concerns.

Each version is given a distinguishing
version number. If the Program
specifies a version number of this License which applies to it and "any
later version", you have the option of following the terms and conditions
either of that version or of any later version published by the Free
Software Foundation. If the Program does not specify a version number of
this License, you may choose any version ever published by the Free Software
Foundation.

10. If you wish to incorporate parts of the Program into other free
programs whose distribution conditions are different, write to the author
to ask for permission. For software which is copyrighted by the Free
Software Foundation, write to the Free Software Foundation; we sometimes
make exceptions for this. Our decision will be guided by the two goals
of preserving the free status of all derivatives of our free software and
of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE,
THERE IS NO WARRANTY
FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES
PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED
OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS
TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE
PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING,

REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR
THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU
General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute
it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this
is what you want to do, use the GNU Lesser General
Public License instead of this License.
KSBA is distributed under mixed GPL and LGPL licenses. Please see the
file AUTHOR for details. The text of the used licenses can be found in
the files:

COPYING.LGPLv3
COPYING.GPLv3
COPYING.GPLv2

1.111 util-linux 2.28.1

1.111.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price.

Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which
gives you legal permission to copy,
distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third

parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work
are not derived from the Program,
and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further

restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will

be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest
possible use to the public, the best way to achieve this is to make it
free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest
to attach them to the start of each source file to most effectively
convey the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU
General Public License as published by
the Free Software Foundation; either version 2 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License along
with this program; if not, write to the Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute
it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this
is what you want to do, use the GNU Lesser General
Public License instead of this License.

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who
decide to use it. You
can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these

rights. These restrictions translate to certain responsibilities for
you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library,
whether gratis
or for a fee, you must give the recipients all the rights that we gave
you. You must make sure that they, too, receive or can get the source
code. If you link other code with the library, you must provide
complete object files to the recipients, so that they can relink them
with the library after making changes to the library and recompiling
it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the
library, and (2) we offer you this license, which gives you legal
permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that
there is no warranty for the free library. Also, if the library is
modified by someone else and passed on, the recipients should know
that what they have is not the original version, so that the original
author's reputation will not be affected by problems that might be
introduced by others.

Finally, software
patents pose a constant threat to the existence of
any free program. We wish to make sure that a company cannot
effectively restrict the users of a free program by obtaining a
restrictive license from a patent holder. Therefore, we insist that
any patent license obtained for a version of the library must be
consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the
ordinary GNU General Public License. This license, the GNU Lesser
General Public License, applies to certain designated libraries, and
is quite different from the ordinary General Public License. We use
this license for certain libraries in order to permit linking those
libraries into non-free programs.

When a program is linked with a library, whether statically or using
a shared library, the combination of the two is legally speaking a
combined work, a derivative of the original library. The ordinary
General Public License therefore permits
such linking only if the
entire combination fits its criteria of freedom. The Lesser General
Public License permits more lax criteria for linking other code with
the library.

We call this license the "Lesser" General Public License because it

does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the

terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be
reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary
GNU General Public
License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the
object code for the work under the terms of Section 6.
Any executables containing that work also fall under Section 6,
whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany
the work with the complete corresponding
machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate
properly with a modified version of the library, if
the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally
distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any
other library
facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to
be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in
certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Library under this License may add
an explicit geographical distribution limitation excluding those countries,
so that distribution is permitted only in or among countries not thus
excluded. In such case, this License incorporates the limitation as if
written in the body of this License.

13. The Free Software Foundation may publish
revised and/or new
versions of the Lesser General Public License from time to time.
Such new versions will be similar in spirit to the present version,
but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library
specifies a version number of this License which applies to it and
"any later version", you have the option of following the terms and
conditions either of that version or of any later version published by
the Free Software Foundation. If the Library does not specify a
license version number, you may choose any version ever published by
the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free
programs whose distribution conditions are incompatible with these,
write to the author to ask for permission. For software which is
copyrighted by the Free Software Foundation, write to the Free
Software Foundation; we sometimes make exceptions for this. Our
decision
will be guided by the two goals of preserving the free status
of all derivatives of our free software and of promoting the sharing
and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO
WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW.
EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR
OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY
KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE
LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME
THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE,
BE LIABLE TO YOU
FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey
the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the library, if
necessary. Here is a sample; alter the names:

 Yoyodyne, Inc., hereby disclaims all copyright interest in the
 library `Frob' (a library for tweaking knobs) written by James Random Hacker.

 <signature of Ty Coon>, 1 April 1990
 Ty Coon, President of Vice

That's all there is to it!
WEV @@ WEV[B "1
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
  notice, and the entire permission notice in its entirety,
  including the disclaimer of warranties.
2. Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote
  products derived from this software without specific prior
  written permission.

THIS SOFTWARE IS PROVIDED ``AS IS" AND ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ALL OF
WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE
LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL
 DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT
OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
USE OF THIS SOFTWARE, EVEN IF NOT ADVISED OF THE POSSIBILITY OF SUCH
DAMAGE.
x   ?"U@,5 @mISmIN<GimCN7g1u|E
43mI,5WEV @@ WEV   @mImImIAmImImI0mImImI*mImI
A0mImImI...
lost+found...

;9GimCN7g

!"#$%&'()*+,-
./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~

!"#$%&'()*+,-
./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~

!"#$%&'()*+,-
./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~

!"#$%&'()*+,-
./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~WEV @@
WEV[B "1
This library is free software; you can redistribute it and/or
modify it under the terms of the Modified BSD License.

The complete text of the license is available in the
../Documentation/licenses/COPYING.BSD-3-Clause file.
Permission to use, copy, modify, and/or distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES
WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR
ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF
OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.
This library is free software; you can redistribute it and/or
modify it under the terms of the GNU Lesser General Public
License as published by the Free Software Foundation; either
version 2.1 of the License, or (at your option) any later
version.

The complete text of the license is available in the
../Documentation/licenses/COPYING.LGPL-2.1-or-later
This library is free software; you can redistribute it and/or
modify it under the terms of the GNU Lesser General Public
License as published by the Free Software Foundation; either
version 2.1 of the License, or (at your option) any later
version.

The complete text of the license is available in the
../Documentation/licenses/COPYING.LGPL-2.1-or-later file.
/*
* Copyright (c) 1989 The Regents of the University of California.
* All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:

* 1. Redistributions of source code must retain the above copyright
*   notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*   notice, this list of conditions and the following disclaimer in the
*   documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*   must display the following acknowledgement:
* This product includes software developed by the University of
* California, Berkeley and its contributors.
* 4. Neither the name of the University nor the names of its contributors
*   may be used to endorse or promote products derived from this software
*
 without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*/

1.112 d-bus 1.10.10

1.112.1 Available under license :

D-Bus is licensed to you under your choice of the Academic Free
License version 2.1, or the GNU General Public License version 2
(or, at your option any later version).

Both licenses are included here. Some of the standalone binaries are
under the GPL only; in particular, but not limited to,
tools/dbus-cleanup-sockets.c and test/decode-gcov.c. Each source code
file is marked with the proper copyright information - if you find a
file that isn't marked please bring it to our attention.

The Academic Free License
v. 2.1

This Academic Free License (the "License") applies to any original work of authorship (the "Original Work") whose owner (the "Licensor") has placed the following notice immediately following the copyright notice for the Original Work:

Licensed under the Academic Free License version 2.1

1) Grant of Copyright License. Licensor hereby grants You a
world-wide, royalty-free, non-exclusive, perpetual, sublicenseable
license to do the following:

a) to reproduce the Original
Work in copies;

b) to prepare derivative works ("Derivative Works") based upon the Original Work;

c) to distribute copies of the Original Work and Derivative Works to the public;

d) to perform the Original Work publicly; and

e) to display the Original Work publicly.

2) Grant of Patent License. Licensor hereby grants You a world-wide,
royalty-free, non-exclusive, perpetual, sublicenseable license, under
patent claims owned or controlled by the Licensor that are embodied in
the Original Work as furnished by the Licensor, to make, use, sell and
offer for sale the Original Work and Derivative Works.

3) Grant of Source Code License. The term "Source Code" means the
preferred form of the Original Work for making modifications to it and
all available documentation describing how to modify the Original
Work. Licensor hereby agrees to provide a machine-readable copy of the
Source Code of the Original Work along with each copy of the Original
Work that Licensor distributes. Licensor reserves
the right to satisfy
this obligation by placing a machine-readable copy of the Source Code
in an information repository reasonably calculated to permit
inexpensive and convenient access by You for as long as Licensor
continues to distribute the Original Work, and by publishing the
address of that information repository in a notice immediately
following the copyright notice that applies to the Original Work.

4) Exclusions From License Grant. Neither the names of Licensor, nor
the names of any contributors to the Original Work, nor any of their
trademarks or service marks, may be used to endorse or promote
products derived from this Original Work without express prior written
permission of the Licensor. Nothing in this License shall be deemed to
grant any rights to trademarks, copyrights, patents, trade secrets or
any other intellectual property of Licensor except as expressly stated
herein. No patent license is granted to make, use, sell or offer to
sell embodiments of any patent claims
other than the licensed claims
defined in Section 2. No right is granted to the trademarks of

Licensor even if such marks are included in the Original Work. Nothing in this License shall be interpreted to prohibit Licensor from licensing under different terms from this License any Original Work that Licensor otherwise would have a right to license.

5) This section intentionally omitted.

6) Attribution Rights. You must retain, in the Source Code of any Derivative Works that You create, all copyright, patent or trademark notices from the Source Code of the Original Work, as well as any notices of licensing and any descriptive text identified therein as an "Attribution Notice." You must cause the Source Code for any Derivative Works that You create to carry a prominent Attribution Notice reasonably calculated to inform recipients that You have modified the Original Work.

7) Warranty of Provenance and Disclaimer of Warranty. Licensor warrants that the copyright in and to the Original Work and the patent rights granted herein by Licensor are owned by the Licensor or are sublicensed to You under the terms of this License with the permission of the contributor(s) of those copyrights and patent rights. Except as expressly stated in the immediately proceeding sentence, the Original Work is provided under this License on an "AS IS" BASIS and WITHOUT WARRANTY, either express or implied, including, without limitation, the warranties of NON-INFRINGEMENT, MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY OF THE ORIGINAL WORK IS WITH YOU. This DISCLAIMER OF WARRANTY constitutes an essential part of this License. No license to Original Work is granted hereunder except under this disclaimer.

8) Limitation of Liability. Under no circumstances and under no legal theory, whether in tort (including negligence), contract, or otherwise, shall the Licensor be liable to any person for any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or the use of the Original Work including, without limitation, damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses. This limitation of liability shall not apply to liability for death or personal injury resulting from Licensor's negligence to the extent applicable law prohibits such limitation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this exclusion and limitation may not apply to You.

9) Acceptance and Termination. If You distribute copies of the Original Work or a Derivative Work, You must make a reasonable effort

under the circumstances to obtain the express assent of recipients to the terms of this License. Nothing else but this License (or another written agreement between Licensor and You) grants You permission to create Derivative Works based upon the Original Work or to exercise any
of the rights granted in Section 1 herein, and any attempt to do so except under the terms of this License (or another written agreement between Licensor and You) is expressly prohibited by U.S. copyright law, the equivalent laws of other countries, and by international treaty. Therefore, by exercising any of the rights granted to You in Section 1 herein, You indicate Your acceptance of this License and all of its terms and conditions.

10) Termination for Patent Action. This License shall terminate automatically and You may no longer exercise any of the rights granted to You by this License as of the date You commence an action, including a cross-claim or counterclaim, against Licensor or any licensee alleging that the Original Work infringes a patent. This termination provision shall not apply for an action alleging patent infringement by combinations of the Original Work with other software or hardware.

11) Jurisdiction, Venue and Governing Law. Any action or suit relating to this
License may be brought only in the courts of a jurisdiction wherein the Licensor resides or in which Licensor conducts its primary business, and under the laws of that jurisdiction excluding its conflict-of-law provisions. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any use of the Original Work outside the scope of this License or after its termination shall be subject to the requirements and penalties of the U.S. Copyright Act, 17 U.S.C. 101 et seq., the equivalent laws of other countries, and international treaty. This section shall survive the termination of this License.

12) Attorneys Fees. In any action to enforce the terms of this License or seeking damages relating thereto, the prevailing party shall be entitled to recover its costs and expenses, including, without limitation, reasonable attorneys' fees and costs incurred in connection with such action, including any appeal of such action. This section
shall survive the termination of this License.

13) Miscellaneous. This License represents the complete agreement concerning the subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable.

14) Definition of "You" in This License. "You" throughout this License, whether in upper or lower case, means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License. For legal entities, "You" includes any entity that controls, is controlled by, or is under common control with you. For purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

15) Right to Use. You may use the Original Work in all ways not otherwise
restricted or conditioned by this License or by law, and
Licensor promises not to interfere with or be responsible for such uses by You.

This license is Copyright (C) 2003-2004 Lawrence E. Rosen. All rights reserved. Permission is hereby granted to copy and distribute this license without modification. This license may not be modified without the express written permission of its copyright owner.

--
END OF ACADEMIC FREE LICENSE. The following is intended to describe the essential differences between the Academic Free License (AFL) version 1.0 and other open source licenses:

The Academic Free License is similar to the BSD, MIT, UoI/NCSA and Apache licenses in many respects but it is intended to solve a few problems with those licenses.

* The AFL is written so as to make it clear what software is being licensed (by the inclusion of a statement following the copyright notice in the software). This way, the license functions better than a template license. The BSD,
MIT and UoI/NCSA licenses apply to unidentified software.

* The AFL contains a complete copyright grant to the software. The BSD and Apache licenses are vague and incomplete in that respect.

* The AFL contains a complete patent grant to the software. The BSD, MIT, UoI/NCSA and Apache licenses rely on an implied patent license and contain no explicit patent grant.

* The AFL makes it clear that no trademark rights are granted to the licensor's trademarks. The Apache license contains such a provision, but the BSD, MIT and UoI/NCSA licenses do not.

* The AFL includes the warranty by the licensor that it either owns the
copyright or that it is distributing the software under a license. None of
the other licenses contain that warranty. All other warranties are disclaimed,
as is the case for the other licenses.

* The AFL is itself copyrighted (with the right granted to copy and distribute
without modification). This ensures that the owner of the copyright to the

license will control changes. The Apache license contains a copyright notice,
but the BSD, MIT and UoI/NCSA licenses do not.
--
START OF GNU GENERAL PUBLIC LICENSE
--

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it. (Some other Free Software Foundation software is covered by
the GNU Library General Public
License instead.) You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price. Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid
anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate to certain responsibilities for you if you
distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program).

Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest
your rights to work written entirely by you; rather, the intent is to
exercise the right to control the distribution of derivative or
collective works based on the Program.

In addition, mere aggregation of another work not based on the Program
with the Program (or with a work based on the Program)
on a volume of
a storage or distribution medium does not bring the other work under
the scope of this License.

3. You may copy and distribute the Program (or a work based on it,
under Section 2) in object code or executable form under the terms of
Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable
source code, which must be distributed under the terms of Sections
1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three
years, to give any third party, for a charge no more than your
cost of physically performing source distribution, a complete
machine-readable copy of the corresponding source code, to be
distributed under the terms of Sections 1 and 2 above on a medium
customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer
to distribute corresponding source code. (This alternative is
allowed only for noncommercial distribution and only if you
received the program in object code or executable form with such
an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for
making modifications to it. For an executable work, complete source
code means all the source code for all modules it contains, plus any
associated interface definition files, plus the scripts used to
control compilation and installation of the executable. However, as a
special exception, the source code distributed need not include
anything that is normally distributed (in either source or binary
form) with the major components (compiler, kernel, and so on) of the
operating system on which the executable runs, unless that component
itself accompanies the executable.

If distribution of executable or object code is made by offering
access to copy from a designated place,
then offering equivalent
access to copy the source code from the same place counts as

distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program),
you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License
and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through
that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the
present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of
software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED
TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software;
you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation; either version 2 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details
type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful
to permit linking proprietary applications with the
library. If this is what you want to do, use the GNU Library General
Public License instead of this License.
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

1. Redistributions of source code must retain the copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products
derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT
OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

1.113 expat 2.2.8

1.113.1 Available under license :

Copyright (c) 1998-2000 Thai Open Source Software Center Ltd and Clark Cooper
Copyright (c) 2001-2017 Expat maintainers

Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be included
in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.
IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY
CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN
ACTION OF CONTRACT,
TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

1.114 avahi 0.7

1.114.1 Available under license :

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts
as the successor of the GNU Library Public License, version 2, hence
the version number 2.1.]

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
Licenses are intended to guarantee your freedom to share and change
free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some
specially designated software packages--typically libraries--of the
Free Software Foundation and other authors who decide
to use it. You
can use it too, but we suggest you first think carefully about whether
this license or the ordinary General Public License is the better
strategy to use in any particular case, based on the explanations
below.

When we speak of free software, we are referring to freedom of use,
not price. Our General Public Licenses are designed to make sure that
you have the freedom to distribute copies of free software (and charge
for this service if you wish); that you receive source code or can get
it if you want it; that you can change the software and use pieces of
it in new free programs; and that you are informed that you can do
these things.

To protect your rights, we need to make restrictions that forbid
distributors to deny you these rights or to ask you to surrender these
rights. These restrictions translate to certain responsibilities for
you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether
gratis
or for a fee, you must give the recipients all the rights that we gave
you. You must make sure that they, too, receive or can get the source
code. If you link other code with the library, you must provide
complete object files to the recipients, so that they can relink them
with the library after making changes to the library and recompiling
it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the

library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the

free library to free
software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to
run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another
language. (Hereinafter, translation is
included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control

compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any

application-supplied function or table used by this function must
be optional: if the application does not supply it, the square
root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably
considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary
GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding

machine-readable source code, which
must be distributed under the terms of Sections 1 and 2 above on a
medium customarily used for software interchange.

If distribution of object code is made by offering access to copy
from a designated place, then offering equivalent access to copy the
source code from the same place satisfies the requirement to
distribute the source code, even though third parties are not
compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the
Library, but is designed to work with the Library by being compiled or
linked with it, is called a "work that uses the Library". Such a
work, in isolation, is not a derivative work of the Library, and
therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library
creates an executable that is a derivative of the Library (because it
contains portions of the Library), rather than a "work that uses
the
library". The executable is therefore covered by this License.
Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file
that is part of the Library, the object code for the work may be a
derivative work of the Library even though the source code is not.
Whether this is true is especially significant if the work can be
linked without the Library, or if the work is itself a library. The
threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data
structure layouts and accessors, and small macros and small inline
functions (ten lines or less in length), then the use of the object
file is unrestricted, regardless of whether it is legally a derivative
work. (Executables containing this object code plus portions of the
Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may
distribute the object
code for the work under the terms of Section 6.
Any executables containing that work also fall under Section 6,
whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or
link a "work that uses the Library" with the Library to produce a
work containing portions of the Library, and distribute that work
under terms of your choice, provided that the terms permit
modification of the work for the customer's own use and reverse

engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the
work with the complete corresponding
machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly
with a modified version of the library, if
the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is

normally
distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any
other library
facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you
do not accept this License. Therefore, by
modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the

Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse
you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system
which is
implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish
revised and/or new
versions of the Lesser General Public License from time to time.
Such new versions will be similar in spirit to the present version,
but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library
specifies a version number of this License which applies to it and
"any later version", you have the option of following the terms and
conditions either of that version or of any later version published by
the Free Software Foundation. If the Library does not specify a
license version number, you may choose any version ever published by
the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free
programs whose distribution conditions are incompatible with these,
write to the author to ask for permission. For software which is
copyrighted by the Free Software Foundation, write to the Free
Software Foundation; we sometimes make exceptions for this. Our
decision will
be guided by the two goals of preserving the free status
of all derivatives of our free software and of promoting the sharing
and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO
WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW.
EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR
OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY
KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE
LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME
THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN
WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY
AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE
LIABLE TO YOU
FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR
CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE
LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING
RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A
FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF
SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH
DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively
convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990

Ty Coon, President of Vice

That's all there is to it!

1.115 netcat 0.7.1

1.115.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it. (Some other Free Software Foundation software is covered by
the GNU Library General Public License instead.) You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price. Our General Public Licenses are designed
to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid
anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate to certain responsibilities for you if you
distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether
gratis or for a fee, you must give the recipients all the rights that
you have. You must make sure that they, too, receive or can get the
source code. And you must show them these terms so they know their
rights.

We protect your rights with two steps: (1) copyright the software, and

(2) offer you this license which gives you legal permission to copy, distribute
and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which
contains
a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies
of the Program's
source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License

along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole
or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered
independent and separate works in
themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of

a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License.

However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that

system; it is up to the author/donor to decide if he or she is willing
to distribute software through
any other system and a licensee cannot
impose that choice.

This section is intended to make thoroughly clear what is believed to
be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in
certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Program under this License
may add an explicit geographical distribution limitation excluding
those countries, so that distribution is permitted only in or among
countries not thus excluded. In such case, this License incorporates
the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions
of the General Public License from time to time. Such new versions will
be similar in spirit to the present version, but may differ in detail to
address new problems or concerns.

Each version is given a distinguishing version number. If the Program
specifies a version number
of this License which applies to it and "any
later version", you have the option of following the terms and conditions
either of that version or of any later version published by the Free
Software Foundation. If the Program does not specify a version number of
this License, you may choose any version ever published by the Free Software
Foundation.

10. If you wish to incorporate parts of the Program into other free
programs whose distribution conditions are different, write to the author
to ask for permission. For software which is copyrighted by the Free
Software Foundation, write to the Free Software Foundation; we sometimes
make exceptions for this. Our decision will be guided by the two goals
of preserving the free status of all derivatives of our free software and
of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY
FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW.
EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES
PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED
OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS
TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE

PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN
IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License,
or
(at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

  Gnomovision version 69, Copyright (C) year name of author
  Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
  This is free software, and you are welcome to redistribute it
  under certain conditions; type `show c' for details.

The hypothetical commands `show w' and
 `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

 Yoyodyne, Inc., hereby disclaims all copyright interest in the program
 `Gnomovision' (which makes passes at compilers) written by James Hacker.

 <signature of Ty Coon>, 1 April 1989
 Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this is what you want to do, use the GNU Library General
Public License instead of this License.

1.116 openssl 1.0.2r

1.116.1 Available under license :

 LICENSE ISSUES
 ==============

 The OpenSSL toolkit stays under a double license, i.e. both the conditions of
 the OpenSSL License and the original SSLeay license apply to the toolkit.
 See below for the actual license texts.

 OpenSSL License

/* ==
* Copyright (c) 1998-2019 The OpenSSL Project. All rights reserved.
*

```
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use
 of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS" AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
 TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
```

* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/

Original SSLeay License

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to. The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code. The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
 *
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
*   notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*   notice, this list of conditions and the following disclaimer in the
*   documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*   must display the following acknowledgement:
*   "This product includes cryptographic software written by
*   Eric Young (eay@cryptsoft.com)"
*   The word 'cryptographic' can be left out if the rouines from the library
*   being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
*   the apps directory (application code) you must include
 an acknowledgement:
*   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*

* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed. i.e. this
 code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place - Suite 330, Boston, MA
02111-1307, USA.
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it. (Some other Free Software Foundation software is covered by
the GNU Library General Public License instead.) You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price.
Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid

anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate to certain responsibilities for you if you
distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether
gratis or for a fee, you must give the recipients all the rights that
you have. You must make sure that they, too, receive or can get the
source code. And you must show them these terms so they know their
rights.

We protect your rights with two steps: (1) copyright the software, and
(2) offer you this license which
gives you legal permission to copy,
distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain
that everyone understands that there is no warranty for this free
software. If the software is modified by someone else and passed on, we
want its recipients to know that what they have is not the original, so
that any problems introduced by others will not reflect on the original
authors' reputations.

Finally, any free program is threatened constantly by software
patents. We wish to avoid the danger that redistributors of a free
program will individually obtain patent licenses, in effect making the
program proprietary. To prevent this, we have made it clear that any
patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and
modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This
License applies to any program or other work which contains
a notice placed by the copyright holder saying it may be distributed
under the terms of this General Public License. The "Program", below,
refers to any such program or work, and a "work based on the Program"
means either the Program or any derivative work under copyright law:
that is to say, a work containing the Program or a portion of it,
either verbatim or with modifications and/or translated into another
language. (Hereinafter, translation is included without limitation in
the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not
covered by this License; they are outside its scope. The act of
running the Program is not restricted, and the output from the Program

is covered only if its contents constitute a work based on the
Program (independent of having been made by running the Program).
Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's
source code as you receive it, in any medium, provided that you
conspicuously and appropriately publish on each copy an appropriate
copyright notice and disclaimer of warranty; keep intact all the
notices that refer to this License and to the absence of any warranty;
and give any other recipients of the Program a copy of this License
along with the Program.

You may charge a fee for the physical act of transferring a copy, and
you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion
of it, thus forming a work based on the Program, and copy and
distribute such modifications or work under the terms of Section 1
above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices
stating that you changed the files and the date of any change.

b) You must cause any work that
you distribute or publish, that in
whole or in part contains or is derived from the Program or any
part thereof, to be licensed as a whole at no charge to all third
parties under the terms of this License.

c) If the modified program normally reads commands interactively
when run, you must cause it, when started running for such
interactive use in the most ordinary way, to print or display an
announcement including an appropriate copyright notice and a
notice that there is no warranty (or else, saying that you provide
a warranty) and that users may redistribute the program under
these conditions, and telling the user how to view a copy of this
License. (Exception: if the Program itself is interactive but
does not normally print such an announcement, your work based on
the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If
identifiable sections of that work are not derived
from the Program,
and can be reasonably considered independent and separate works in
themselves, then this License, and its terms, do not apply to those
sections when you distribute them as separate works. But when you
distribute the same sections as part of a whole which is a work based
on the Program, the distribution of the whole must be on the terms of

this License, whose permissions for other licensees extend to the
entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest
your rights to work written entirely by you; rather, the intent is to
exercise the right to control the distribution of derivative or
collective works based on the Program.

In addition, mere aggregation of another work not based on the Program
with the Program (or with a work based on the Program) on a volume of
a storage or distribution medium does not bring the other work under
the scope of this License.

3. You may
copy and distribute the Program (or a work based on it,
under Section 2) in object code or executable form under the terms of
Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable
source code, which must be distributed under the terms of Sections
1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three
years, to give any third party, for a charge no more than your
cost of physically performing source distribution, a complete
machine-readable copy of the corresponding source code, to be
distributed under the terms of Sections 1 and 2 above on a medium
customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer
to distribute corresponding source code. (This alternative is
allowed only for noncommercial distribution and only if
you
received the program in object code or executable form with such
an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for
making modifications to it. For an executable work, complete source
code means all the source code for all modules it contains, plus any
associated interface definition files, plus the scripts used to
control compilation and installation of the executable. However, as a
special exception, the source code distributed need not include
anything that is normally distributed (in either source or binary
form) with the major components (compiler, kernel, and so on) of the
operating system on which the executable runs, unless that component
itself accompanies the executable.

If distribution of executable or object code is made by offering

access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even
though third parties are not
compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying
the
Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if
a patent
license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to

apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM,
TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE
PROGRAM TO OPERATE WITH ANY OTHER
PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Appendix: How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) 19yy <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free
Software Foundation; either version 2 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of

MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19yy name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c'
for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this is what you want to do, use the GNU Library General
Public
License instead of this License.

The "Artistic License"

Preamble

The intent of this document is to state the conditions under which a

Package may be copied, such that the Copyright Holder maintains some
semblance of artistic control over the development of the package,
while giving the users of the package the right to use and distribute
the Package in a more-or-less customary fashion, plus the right to make
reasonable modifications.

Definitions:

"Package" refers to the collection of files distributed by the
Copyright Holder, and derivatives of that collection of files
created through textual modification.

"Standard Version" refers to such a Package if it has not been
modified, or has been modified in accordance with the wishes
of the Copyright Holder as specified below.

"Copyright Holder" is whoever is named in the copyright or
copyrights for the package.

"You" is you, if you're thinking about copying or distributing
this Package.

"Reasonable copying fee" is whatever you can justify on the
basis
of media cost, duplication charges, time of people involved,
and so on. (You will not be required to justify it to the
Copyright Holder, but only to the computing community at large
as a market that must bear the fee.)

"Freely Available" means that no fee is charged for the item
itself, though there may be fees involved in handling the item.
It also means that recipients of the item may redistribute it
under the same conditions they received it.

1. You may make and give away verbatim copies of the source form of the
Standard Version of this Package without restriction, provided that you
duplicate all of the original copyright notices and associated disclaimers.

2. You may apply bug fixes, portability fixes and other modifications
derived from the Public Domain or from the Copyright Holder. A Package
modified in such a way shall still be considered the Standard Version.

3. You may otherwise modify your copy of this Package in any way, provided
that you insert a prominent
notice in each changed file stating how and
when you changed that file, and provided that you do at least ONE of the
following:

a) place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major archive site such as uunet.uu.net, or by allowing the Copyright Holder to include your modifications in the Standard Version of the Package.

b) use the modified Package only within your corporation or organization.

c) rename any non-standard executables so the names do not conflict with standard executables, which must also be provided, and provide a separate manual page for each non-standard executable that clearly documents how it differs from the Standard Version.

d) make other distribution arrangements with the Copyright Holder.

4. You may distribute the programs of this Package in object code or executable
form, provided that you do at least ONE of the following:

a) distribute a Standard Version of the executables and library files, together with instructions (in the manual page or equivalent) on where to get the Standard Version.

b) accompany the distribution with the machine-readable source of the Package with your modifications.

c) give non-standard executables non-standard names, and clearly document the differences in manual pages (or equivalent), together with instructions on where to get the Standard Version.

d) make other distribution arrangements with the Copyright Holder.

5. You may charge a reasonable copying fee for any distribution of this Package. You may charge any fee you choose for support of this Package. You may not charge a fee for this Package itself. However, you may distribute this Package in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution provided
that you do not advertise this Package as a
product of your own. You may embed this Package's interpreter within an executable of yours (by linking); this shall be construed as a mere form of aggregation, provided that the complete Standard Version of the interpreter is so embedded.

6. The scripts and library files supplied as input to or produced as output from the programs of this Package do not automatically fall under the copyright of this Package, but belong to whoever generated them, and may be sold commercially, and may be aggregated with this

Package. If such scripts or library files are aggregated with this
Package via the so-called "undump" or "unexec" methods of producing a
binary executable image, then distribution of such an image shall
neither be construed as a distribution of this Package nor shall it
fall under the restrictions of Paragraphs 3 and 4, provided that you do
not represent such an executable image as a Standard Version of this
Package.

7. C subroutines
 (or comparably compiled subroutines in other
languages) supplied by you and linked into this Package in order to
emulate subroutines and variables of the language defined by this
Package shall not be considered part of this Package, but are the
equivalent of input as in Paragraph 6, provided these subroutines do
not change the language in any way that would cause it to fail the
regression tests for the language.

8. Aggregation of this Package with a commercial distribution is always
permitted provided that the use of this Package is embedded; that is,
when no overt attempt is made to make this Package's interfaces visible
to the end user of the commercial distribution. Such use shall not be
construed as a distribution of this Package.

9. The name of the Copyright Holder may not be used to endorse or promote
products derived from this software without specific prior written permission.

10. THIS PACKAGE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, WITHOUT
 LIMITATION, THE IMPLIED
WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The End

1.117 libnl3 3.2.28

1.117.1 Available under license :

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts
as the successor of the GNU Library Public License, version 2, hence
the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software
patents pose a constant threat to the existence of
any free program. We wish to make sure that a company cannot
effectively restrict the users of a free program by obtaining a
restrictive license from a patent holder. Therefore, we insist that
any patent license obtained for a version of the library must be
consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the
ordinary GNU General Public License. This license, the GNU Lesser
General Public License, applies to certain designated libraries, and
is quite different from the ordinary General Public License. We use
this license for certain libraries in order to permit linking those
libraries into non-free programs.

When a program is linked with a library, whether statically or using
a shared library, the combination of the two is legally speaking a
combined work, a derivative of the original library. The ordinary
General Public License therefore permits
such linking only if the
entire combination fits its criteria of freedom. The Lesser General
Public License permits more lax criteria for linking other code with
the library.

We call this license the "Lesser" General Public License because it
does Less to protect the user's freedom than the ordinary General
Public License. It also provides other free software developers Less
of an advantage over competing non-free programs. These disadvantages
are the reason we use the ordinary General Public License for many
libraries. However, the Lesser license provides advantages in certain
special circumstances.

For example, on rare occasions, there may be a special need to
encourage the widest possible use of a certain library, so that it becomes
a de-facto standard. To achieve this, non-free programs must be
allowed to use the library. A more frequent case is that a free
library does the same job as widely used non-free libraries. In this
case, there is little to gain by limiting
the free library to free
software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free
programs enables a greater number of people to use a large body of
free software. For example, permission to use the GNU C Library in
non-free programs enables many more people to use the whole GNU
operating system, as well as its variant, the GNU/Linux operating
system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those

sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany
the work with the complete corresponding
machine-readable source code for the Library including whatever
changes were used in the work (which must be distributed under
Sections 1 and 2 above); and, if the work is an executable linked
with the Library, with the complete machine-readable "work that
uses the Library", as object code and/or source code, so that the
user can modify the Library and then relink to produce a modified
executable containing the modified Library. (It is understood
that the user who changes the contents of definitions files in the
Library will not necessarily be able to recompile the application
to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the
Library. A suitable mechanism is one that (1) uses at run time a
copy of the library already present on the user's computer system,
rather than copying library functions into the executable, and (2)
will operate
properly with a modified version of the library, if
the user installs one, as long as the modified version is
interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at
least three years, to give the same user the materials
specified in Subsection 6a, above, for a charge no more
than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy
from a designated place, offer equivalent access to copy the above
specified materials from the same place.

e) Verify that the user has already received a copy of these
materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the
Library" must include any data and utility programs needed for
reproducing the executable from it. However, as a special exception,
the materials to be distributed need not include anything that is
normally
distributed (in either source or binary form) with the major
components (compiler, kernel, and so on) of the operating system on
which the executable runs, unless that component itself accompanies
the executable.

It may happen that this requirement contradicts the license
restrictions of other proprietary libraries that do not normally
accompany the operating system. Such a contradiction means you cannot
use both them and the Library together in an executable that you

distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or

otherwise) that contradict the conditions of this License, they do not excuse
you from the conditions of this License. If you cannot
distribute so as to satisfy simultaneously your obligations under this
License and any other pertinent obligations, then as a consequence you
may not distribute the Library at all. For example, if a patent
license would not permit royalty-free redistribution of the Library by
all those who receive copies directly or indirectly through you, then
the only way you could satisfy both it and this License would be to
refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any
particular circumstance, the balance of the section is intended to apply,
and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any
patents or other property right claims or to contest validity of any
such claims; this section has the sole purpose of protecting the
integrity of the free software distribution system
which is
implemented by public license practices. Many people have made
generous contributions to the wide range of software distributed
through that system in reliance on consistent application of that
system; it is up to the author/donor to decide if he or she is willing
to distribute software through any other system and a licensee cannot
impose that choice.

This section is intended to make thoroughly clear what is believed to
be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in
certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Library under this License may add
an explicit geographical distribution limitation excluding those countries,
so that distribution is permitted only in or among countries not thus
excluded. In such case, this License incorporates the limitation as if
written in the body of this License.

13. The Free Software Foundation may publish
revised and/or new
versions of the Lesser General Public License from time to time.
Such new versions will be similar in spirit to the present version,
but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library
specifies a version number of this License which applies to it and
"any later version", you have the option of following the terms and
conditions either of that version or of any later version published by

the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision
will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE,
BE LIABLE TO YOU
FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey
the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we

stand
ready to extend this provision to those domains in future versions
of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents.
States should not allow patents to restrict development and use of
software on general-purpose computers, but in those that do, we wish to
avoid the special danger that patents applied to a free program could
make it effectively proprietary. To prevent this, the GPL assures that
patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and
modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of
works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this
License. Each licensee is addressed as "you". "Licensees"
and
"recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work
in a fashion requiring copyright permission, other than the making of an
exact copy. The resulting work is called a "modified version" of the
earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based
on the Program.

To "propagate" a work means to do anything with it that, without
permission, would make you directly or secondarily liable for
infringement under applicable copyright law, except executing it on a
computer or modifying a private copy. Propagation includes copying,
distribution (with or without modification), making available to the
public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other
parties to make or receive copies. Mere interaction with a user through
a computer network, with no transfer of a copy, is
not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The
"System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally
available free
programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding

Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered
by this License only if the output, given its
content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed;
section 10
makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately
publish on each copy an appropriate copyright notice;
keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to
"keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution
medium, is called an
"aggregate" if the compilation and its resulting copyright are not

used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is

available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates

for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or

authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on

those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above
requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is

reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright
holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights
granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that

any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or

arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License,

section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE

USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17.
Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>
This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program
into proprietary programs. If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library. If this is what you want to
do, use the GNU Lesser General
Public License instead of this License. But first, please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.

1.118 golang 1.8.1

1.118.1 Available under license :

Copyright (c) 2009 The Go Authors. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are
met:

* Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above
copyright notice, this list of conditions and the following disclaimer
in the documentation and/or other materials provided with the
distribution.
* Neither the name of Google Inc. nor the names of its
contributors may be used to endorse or promote products derived from
this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT

LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER
OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

1.119 efivar 0.24

1.119.1 Available under license :

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts
as the successor of the GNU Library Public License, version 2, hence
the version number 2.1.]

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
Licenses are intended to guarantee your freedom to share and change
free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some
specially designated software packages--typically libraries--of the
Free Software Foundation and other authors who decide to use it. You
can use it too, but we suggest you first think carefully about whether
this
license or the ordinary General Public License is the better
strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use,
not price. Our General Public Licenses are designed to make sure that
you have the freedom to distribute copies of free software (and charge
for this service if you wish); that you receive source code or can get
it if you want it; that you can change the software and use pieces of
it in new free programs; and that you are informed that you can do
these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public

License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice
and disclaimer of warranty; keep intact
all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table
of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do
not apply to those
sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you
must alter all the notices that refer to this License, so
that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the

ordinary GNU General Public License has appeared, then you can specify
that version instead if you wish.) Do not make any other change in
these notices.

Once this change is made in a given copy, it is irreversible for
that copy, so the ordinary GNU General Public License applies to all
subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of
the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or
derivative of it, under Section 2) in object code or executable form
under the terms of Sections 1 and 2 above provided that you accompany
it with the complete corresponding machine-readable source code, which
must be distributed under the terms of Sections 1 and 2
above on a
medium customarily used for software interchange.

If distribution of object code is made by offering access to copy
from a designated place, then offering equivalent access to copy the
source code from the same place satisfies the requirement to
distribute the source code, even though third parties are not
compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the
Library, but is designed to work with the Library by being compiled or
linked with it, is called a "work that uses the Library". Such a
work, in isolation, is not a derivative work of the Library, and
therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library
creates an executable that is a derivative of the Library (because it
contains portions of the Library), rather than a "work that uses the
library". The executable is therefore covered by this License.
Section 6 states terms for distribution
of such executables.

When a "work that uses the Library" uses material from a header file
that is part of the Library, the object code for the work may be a
derivative work of the Library even though the source code is not.
Whether this is true is especially significant if the work can be
linked without the Library, or if the work is itself a library. The
threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data
structure layouts and accessors, and small macros and small inline
functions (ten lines or less in length), then the use of the object

file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6,
whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version
is
interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials

specified in Subsection 6a, above, for a charge no more
than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy
from a designated place, offer equivalent access to copy the above
specified materials from the same place.

e) Verify that the user has already received a copy of these
materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the
Library" must include any data and utility programs needed for
reproducing the executable from it. However, as a special exception,
the materials to be distributed need not include anything that is
normally distributed (in either source or binary form) with the major
components (compiler, kernel, and so
on) of the operating system on
which the executable runs, unless that component itself accompanies
the executable.

It may happen that this requirement contradicts the license
restrictions of other proprietary libraries that do not normally
accompany the operating system. Such a contradiction means you cannot
use both them and the Library together in an executable that you
distribute.

7. You may place library facilities that are a work based on the
Library side-by-side in a single library together with other library
facilities not covered by this License, and distribute such a combined
library, provided that the separate distribution of the work based on
the Library and of the other library facilities is otherwise
permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work
based on the Library, uncombined with any other library
facilities. This must be distributed under the terms of the
Sections above.

b) Give prominent notice with the combined library of the fact
that part of it is a work based on the Library, and explaining
where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute
the Library except as expressly provided under this License. Any
attempt otherwise to copy, modify, sublicense, link with, or
distribute the Library is void, and will automatically terminate your
rights under this License. However, parties who have received copies,

or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing

to distribute software through any other system and a licensee cannot
impose that choice.

This section is intended to make thoroughly clear what is believed to
be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in
certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Library under this License may add
an explicit geographical distribution limitation excluding those countries,
so that distribution is permitted only in or among countries not thus
excluded. In such case, this License incorporates the limitation as if
written in the body of this License.

13. The Free Software Foundation may publish revised and/or new
versions of the Lesser General Public License from time to time.
Such new versions
will be similar in spirit to the present version,
but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library
specifies a version number of this License which applies to it and
"any later version", you have the option of following the terms and
conditions either of that version or of any later version published by
the Free Software Foundation. If the Library does not specify a
license version number, you may choose any version ever published by
the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free
programs whose distribution conditions are incompatible with these,
write to the author to ask for permission. For software which is
copyrighted by the Free Software Foundation, write to the Free
Software Foundation; we sometimes make exceptions for this. Our
decision will be guided by the two goals of preserving the free status
of all derivatives of our free software and
of promoting the sharing
and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO
WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW.
EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR
OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY
KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE
LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME

THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE
LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your

school, if any, to sign a "copyright disclaimer" for
 the library, if
necessary. Here is a sample; alter the names:

 Yoyodyne, Inc., hereby disclaims all copyright interest in the
 library `Frob' (a library for tweaking knobs) written by James Random Hacker.

 <signature of Ty Coon>, 1 April 1990
 Ty Coon, President of Vice

That's all there is to it!

1.120 policycoreutils 2.6

1.120.1 Available under license :

GNU GENERAL PUBLIC LICENSE
        Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

       Preamble

 The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it. (Some other Free Software Foundation software is covered by
the GNU Lesser General Public License instead.)
  You can apply it to
your programs, too.

 When we speak of free software, we are referring to freedom, not
price. Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

 To protect your rights, we need to make restrictions that forbid
anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate to certain responsibilities for you if you
distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program).

Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the

entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest
your rights to work written entirely by you; rather, the intent is to
exercise the right to control the distribution of derivative or
collective works based on the Program.

In addition, mere aggregation
of another work not based on the Program
with the Program (or with a work based on the Program) on a volume of
a storage or distribution medium does not bring the other work under
the scope of this License.

3. You may copy and distribute the Program (or a work based on it,
under Section 2) in object code or executable form under the terms of
Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable
source code, which must be distributed under the terms of Sections
1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three
years, to give any third party, for a charge no more than your
cost of physically performing source distribution, a complete

machine-readable copy of the corresponding source code, to be
distributed under the terms of Sections 1 and 2 above on a medium
customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer
to distribute corresponding source code. (This alternative is
allowed only for noncommercial distribution and only if you
received the program in object code or executable form with such
an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for
making modifications to it. For an executable work, complete source
code means all the source code for all modules it contains, plus any
associated interface definition files, plus the scripts used to
control compilation and installation of the executable. However, as a

special exception, the source code distributed need not include
anything that is normally distributed (in either source or binary
form) with the major components (compiler, kernel, and so on) of the
operating system on which the executable runs, unless that component
itself accompanies the executable.

If distribution of executable or object code is made by offering

access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License.
However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to

apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author

to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option)
any later version.

This program is distributed in the hope that it will be useful,

but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License along
with this program; if not, write to the Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.
This
is free software, and you are welcome to redistribute it
under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than 'show w' and 'show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
'Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General
Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this is what you want to do, use the GNU Lesser General
Public License instead of this License.

1.121 sysklogd 1.5.1

1.121.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
675 Mass Ave, Cambridge, MA 02139, USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to

using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work

which contains
a notice placed by the copyright holder saying it may be distributed
under the terms of this General Public License. The "Program", below,
refers to any such program or work, and a "work based on the Program"
means either the Program or any derivative work under copyright law:
that is to say, a work containing the Program or a portion of it,
either verbatim or with modifications and/or translated into another
language. (Hereinafter, translation is included without limitation in
the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not
covered by this License; they are outside its scope. The act of
running the Program is not restricted, and the output from the Program
is covered only if its contents constitute a work based on the
Program (independent of having been made by running the Program).
Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim
copies of the Program's
source code as you receive it, in any medium, provided that you
conspicuously and appropriately publish on each copy an appropriate
copyright notice and disclaimer of warranty; keep intact all the
notices that refer to this License and to the absence of any warranty;
and give any other recipients of the Program a copy of this License
along with the Program.

You may charge a fee for the physical act of transferring a copy, and
you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion
of it, thus forming a work based on the Program, and copy and
distribute such modifications or work under the terms of Section 1
above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices
stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in
whole
or in part contains or is derived from the Program or any
part thereof, to be licensed as a whole at no charge to all third
parties under the terms of this License.

c) If the modified program normally reads commands interactively
when run, you must cause it, when started running for such
interactive use in the most ordinary way, to print or display an
announcement including an appropriate copyright notice and a
notice that there is no warranty (or else, saying that you provide

a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code

or executable form with such
an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy
the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6.
Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent

infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number

of this License which applies to it and "any
later version", you have the option of following the terms and conditions
either of that version or of any later version published by the Free
Software Foundation. If the Program does not specify a version number of
this License, you may choose any version ever published by the Free Software
Foundation.

10. If you wish to incorporate parts of the Program into other free
programs whose distribution conditions are different, write to the author
to ask for permission. For software which is copyrighted by the Free
Software Foundation, write to the Free Software Foundation; we sometimes
make exceptions for this. Our decision will be guided by the two goals
of preserving the free status of all derivatives of our free software and
of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY
FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE
LAW. EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES
PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED
OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS
TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE
PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING,
REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING
WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR
REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES,
INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING
OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED
TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY
YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER
PROGRAMS),
EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE
POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Appendix: How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest
possible use to the public, the best way to achieve this is to make it
free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest

to attach them to the start of each source file to most effectively
convey the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) 19yy <name of author>

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation; either version 2 of
the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19yy name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c'
should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this is what you want to do, use the GNU Library General
Public License instead of this License.

1.122 base-passwd 3.5.3

1.122.1 Available under license :

Format-Specification: http://svn.debian.org/wsvn/dep/web/deps/dep5.mdwn?op=file&rev=135
Name: base-passwd
Maintainer: Colin Watson <cjwatson@debian.org>

Files: update-passwd.c, man/*
Copyright: Copyright 1999-2002 Wichert Akkerman <wichert@deephackmode.org>
Copyright 2002, 2003, 2004 Colin Watson <cjwatson@debian.org>
License: GPL-2

Files: passwd.master, group.master
License: PD
X-Notes: Originally written by Ian Murdock <imurdock@debian.org> and
Bruce Perens <bruce@pixar.com>.

Files: doc/*
Copyright: Copyright 2001, 2002 Joey Hess
Copyright 2002, 2003, 2004, 2005, 2007 Colin Watson
Copyright 2007 David Mandelberg
License: GPL-2

License: GPL-2
On Debian and Debian-based systems, a copy of the GNU General Public
License version 2 is available in /usr/share/common-licenses/GPL-2.
    GNU GENERAL PUBLIC LICENSE
      Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
                51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

     Preamble

 The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software

Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program
or other work which contains
a notice placed by the copyright holder saying it may be distributed
under the terms of this General Public License. The "Program", below,
refers to any such program or work, and a "work based on the Program"
means either the Program or any derivative work under copyright law:
that is to say, a work containing the Program or a portion of it,
either verbatim or with modifications and/or translated into another
language. (Hereinafter, translation is included without limitation in
the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not
covered by this License; they are outside its scope. The act of
running the Program is not restricted, and the output from the Program
is covered only if its contents constitute a work based on the
Program (independent of having been made by running the Program).
Whether that is true depends on what the Program does.

1. You may copy and distribute
verbatim copies of the Program's
source code as you receive it, in any medium, provided that you
conspicuously and appropriately publish on each copy an appropriate
copyright notice and disclaimer of warranty; keep intact all the
notices that refer to this License and to the absence of any warranty;
and give any other recipients of the Program a copy of this License
along with the Program.

You may charge a fee for the physical act of transferring a copy, and
you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion
of it, thus forming a work based on the Program, and copy and
distribute such modifications or work under the terms of Section 1
above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices
stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish,
that in
whole or in part contains or is derived from the Program or any
part thereof, to be licensed as a whole at no charge to all third
parties under the terms of this License.

c) If the modified program normally reads commands interactively
when run, you must cause it, when started running for such
interactive use in the most ordinary way, to print or display an
announcement including an appropriate copyright notice and a

notice that there is no warranty (or else, saying that you provide
a warranty) and that users may redistribute the program under
these conditions, and telling the user how to view a copy of this
License. (Exception: if the Program itself is interactive but
does not normally print such an announcement, your work based on
the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If
identifiable sections of that work are not derived from the Program,
and can
be reasonably considered independent and separate works in
themselves, then this License, and its terms, do not apply to those
sections when you distribute them as separate works. But when you
distribute the same sections as part of a whole which is a work based
on the Program, the distribution of the whole must be on the terms of
this License, whose permissions for other licensees extend to the
entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest
your rights to work written entirely by you; rather, the intent is to
exercise the right to control the distribution of derivative or
collective works based on the Program.

In addition, mere aggregation of another work not based on the Program
with the Program (or with a work based on the Program) on a volume of
a storage or distribution medium does not bring the other work under
the scope of this License.

3. You may copy and distribute the Program
(or a work based on it,
under Section 2) in object code or executable form under the terms of
Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable
source code, which must be distributed under the terms of Sections
1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three
years, to give any third party, for a charge no more than your
cost of physically performing source distribution, a complete
machine-readable copy of the corresponding source code, to be
distributed under the terms of Sections 1 and 2 above on a medium
customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer
to distribute corresponding source code. (This alternative is
allowed only for noncommercial distribution and only if you
received the program

in object code or executable form with such
an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled
to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based
on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent

infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit
royalty-free redistribution of the Program by
all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute
software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies

a version number of this License which applies to it and "any
later version", you have the option of following the terms and conditions
either of that version or of any later version published by the Free
Software Foundation. If the Program does not specify a version number of
this License, you may choose any version ever published by the Free Software
Foundation.

10. If you wish to incorporate parts of the Program into other free
programs whose distribution conditions are different, write to the author
to ask for permission. For software which is copyrighted by the Free
Software Foundation, write to the Free Software Foundation; we sometimes
make exceptions for this. Our decision will be guided by the two goals
of preserving the free status of all derivatives of our free software and
of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY
FOR THE PROGRAM, TO THE EXTENT PERMITTED
BY APPLICABLE LAW. EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES
PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED
OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS
TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE
PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING,
REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING
WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR
REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES,
INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING
OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED
TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY
YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY
OTHER
PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE
POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest
possible use to the public, the best way to achieve this is to make it
free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest

to attach them to the start of each source file to most effectively
convey the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation; either version
2 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical
commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

1.123 ipmi-tool 1.8.15

1.123.1 Available under license :

Copyright (c) 2003 Sun Microsystems, Inc. All Rights Reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistribution of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistribution in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Sun Microsystems, Inc. or the names of contributors may be used to endorse or promote products derived from this software without specific prior written permission.

This software is provided "AS IS," without a warranty of any kind.
ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE HEREBY EXCLUDED.
SUN MICROSYSTEMS,
INC. ("SUN") AND ITS LICENSORS SHALL NOT BE LIABLE
FOR ANY DAMAGES SUFFERED BY LICENSEE AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THIS SOFTWARE OR ITS DERIVATIVES. IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR DIRECT, INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF THE USE OF OR INABILITY TO USE THIS SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

1.124 u-boot 2016.07

1.124.1 Available under license :

Redistribution and use in source and binary forms, with or
without modification, are permitted provided that the following
conditions are met:

1. Redistributions of source code must retain the above
   copyright notice, this list of conditions and the following
   disclaimer.
2. Redistributions in binary form must reproduce the above
   copyright notice, this list of conditions and the following
   disclaimer in the documentation and/or other materials
   provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND
CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE,
EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

GPL License Exception:

Even though U-Boot in general is covered by the GPL-2.0/GPL-2.0+,
this does *not* cover the so-called "standalone" applications that
use U-Boot services by means of the jump table provided by U-Boot
exactly for this purpose - this is merely considered normal use of
U-Boot, and does *not* fall under the heading of "derived work".

The header files "include/image.h" and "arch/*/include/asm/u-boot.h"
define interfaces to U-Boot. Including these (unmodified) header
files in another file is considered normal use of U-Boot, and does
not fall under the heading of "derived work".
-- Wolfgang Denk
Copyright (c) 2010, Andrey Makarov (makarov@bmstu.ru, mka-at-mailru@mail.ru),
with Reserved Font Name Anka/Coder Narrow.

Copyright (c) 2011, Pablo Impallari (www.impallari.com|impallari@gmail.com),
Rodrigo Fuenzalida (www.rfuenzalida.com) with Reserved Font Name Cantora.

This Font Software is licensed under the SIL Open Font License, Version 1.1.

This license is copied below, and is also available with a FAQ at:
http://scripts.sil.org/OFL

SIL OPEN FONT LICENSE Version 1.1 - 26 February 2007

PREAMBLE
The goals of the Open Font License (OFL) are to stimulate worldwide development of collaborative font projects, to support the font creation efforts of academic and linguistic communities, and to provide a free and open framework in which fonts may be shared and improved in partnership with others.

The OFL allows the licensed fonts to be used, studied, modified and redistributed
freely as long as they are not sold by themselves. The
fonts, including any derivative works, can be bundled, embedded, redistributed and/or sold with any software provided that any reserved names are not used by derivative works. The fonts and derivatives, however, cannot be released under any other type of license. The requirement for fonts to remain under this license does not apply to any document created using the fonts or their derivatives.

DEFINITIONS
"Font Software" refers to the set of files released by the Copyright Holder(s) under this license and clearly marked as such. This may include source files, build scripts and documentation.

"Reserved Font Name" refers to any names specified as such after the copyright statement(s).

"Original Version" refers to the collection of Font Software components as distributed by the Copyright Holder(s).

"Modified Version" refers to any derivative made by adding to, deleting, or substituting -- in part or in whole -- any of the
components of the
Original Version, by changing formats or by porting the Font Software to a new environment.

"Author" refers to any designer, engineer, programmer, technical writer or other person who contributed to the Font Software.

PERMISSION & CONDITIONS
Permission is hereby granted, free of charge, to any person obtaining a copy of the Font Software, to use, study, copy, merge, embed, modify,

redistribute, and sell modified and unmodified copies of the Font Software, subject to the following conditions:

1) Neither the Font Software nor any of its individual components, in Original or Modified Versions, may be sold by itself.

2) Original or Modified Versions of the Font Software may be bundled, redistributed and/or sold with any software, provided that each copy contains the above copyright notice and this license. These can be included either as stand-alone text files, human-readable headers or in the appropriate machine-readable metadata fields within text or binary files
as long as those fields can be easily viewed by the user.

3) No Modified Version of the Font Software may use the Reserved Font Name(s) unless explicit written permission is granted by the corresponding Copyright Holder. This restriction only applies to the primary font name as presented to the users.

4) The name(s) of the Copyright Holder(s) or the Author(s) of the Font Software shall not be used to promote, endorse or advertise any Modified Version, except to acknowledge the contribution(s) of the Copyright Holder(s) and the Author(s) or with their explicit written permission.

5) The Font Software, modified or unmodified, in part or in whole, must be distributed entirely under this license, and must not be distributed under any other license. The requirement for fonts to remain under this license does not apply to any document created using the Font Software.

TERMINATION
This license becomes null and void if any of the above conditions are not met.

DISCLAIMER
THE FONT SOFTWARE
IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.
ISC License:
Copyright (c) 2004-2010 by Internet Systems Consortium, Inc. ("ISC")

Copyright (c) 1995-2003 by Internet Software Consortium

Permission to use, copy, modify, and/or distribute this software
for any purpose with or without fee is hereby granted,
provided that the above copyright notice and this permission notice
appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES
WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE
FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR
ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS,
WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION,
ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF
THIS SOFTWARE.
This source code has been made available to you by IBM on an AS-IS
basis. Anyone receiving this source is licensed under IBM
copyrights to use it in any way he or she deems fit, including
copying it, modifying it, compiling it, and redistributing it either
with or without modifications. No license under IBM patents or
patent applications is to be implied by the copyright license.

Any user of this software should understand that IBM cannot provide
technical support for this software and will not be responsible for
any consequences resulting from the use of this software.

Any person who transfers this source code or any derivative work
must include the IBM copyright notice, this paragraph, and the
preceding two paragraphs in the transferred software.

COPYRIGHT I B M CORPORATION 1995
LICENSED MATERIAL - PROGRAM PROPERTY OF I B M
License

LZMA SDK is placed in the public domain.
The files in this directory and elsewhere which refer to this LICENCE
file are part of JFFS2, the Journalling Flash File System v2.

Copyright 2001-2007 Red Hat, Inc. and others

JFFS2 is free software; you can redistribute it and/or modify it under
the terms of the GNU General Public License as published by the Free
Software Foundation; either version 2 or (at your option) any later
version.

JFFS2 is distributed in the hope that it will be useful, but WITHOUT
ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or
FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License

for more details.

You should have received a copy of the GNU General Public License along
with JFFS2; if not, write to the Free Software Foundation, Inc.,
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.

As a special exception, if other files instantiate templates or use
macros or inline functions from these files, or you compile these
files and link them with other works to produce
a work based on these
files, these files do not by themselves cause the resulting work to be
covered by the GNU General Public License. However the source code for
these files must still be made available in accordance with section (3)
of the GNU General Public License.

This exception does not invalidate any other reasons why a work based on
this file might be covered by the GNU General Public License.
Note that this license is not endorsed by the Free Software Foundation.
It is available here as a convenience to readers of [1]the license
list.

The eCos license version 2.0

This file is part of eCos, the Embedded Configurable Operating System.
Copyright (C) 1998, 1999, 2000, 2001, 2002 Red Hat, Inc.

eCos is free software; you can redistribute it and/or modify it under
the terms of the GNU General Public License as published by the Free
Software Foundation; either version 2 or (at your option) any later
version.

eCos is distributed in the hope that it will be useful, but WITHOUT ANY
WARRANTY; without even the implied warranty of MERCHANTABILITY or
FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License
for more details.

You should have received a copy of the GNU General Public License along
with eCos; if not, write to the Free Software Foundation, Inc., 51
Franklin St, Fifth Floor, Boston, MA 02110-1301 USA.

As a special
exception, if other files instantiate templates or use
macros or inline functions from this file, or you compile this file and
link it with other works to produce a work based on this file, this
file does not by itself cause the resulting work to be covered by the
GNU General Public License. However the source code for this file must
still be made available in accordance with section (3) of the GNU
General Public License.

This exception does not invalidate any other reasons why a work based on this file might be covered by the GNU General Public License.

Alternative licenses for eCos may be arranged by contacting Red Hat, Inc. at http://sources.redhat.com/ecos/ecos-license/

####ECOSGPLCOPYRIGHTEND####

References

1. http://www.gnu.org/licenses/license-list.html

GNU LIBRARY GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the library GPL. It is
numbered 2 because it goes with version 2 of the ordinary GPL.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some specially designated Free Software Foundation software, and to any other libraries whose authors decide to use it. You can use it for your libraries, too.

When
we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library, or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link a program with the library, you must provide complete object files to the recipients so that they can relink them with the library, after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

Our method of protecting your rights has two steps: (1) copyright the library, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the library.

Also, for each distributor's protection, we want to make certain that everyone understands that there is no warranty for this free library. If the library is modified by someone else and passed on, we want its recipients to know that what they have is not the original version, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that companies distributing free software will individually obtain patent licenses, thus in effect transforming the program into proprietary software. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License, which was designed for utility programs. This license, the GNU Library General Public License, applies to certain designated libraries. This license is quite different from the ordinary one; be sure to read it in full, and don't assume that anything in it is the same as in the ordinary license.

The reason we have a separate public license for some libraries is that they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and legal sense, the linked executable is a combined work, a derivative of the original library, and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public License for libraries did not effectively promote software

sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification
follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

GNU LIBRARY GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below,
refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated

interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if
its contents constitute a work based
on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you
also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the

application. Therefore, Subsection 2d requires
that any
application-supplied function or table used by this function must
be optional: if the application does not supply it, the square
root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution
of derivative or
collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which

must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also compile or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

c) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

d) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you

distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or

otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other
pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through
that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Library General Public License from time to time. Such new versions will be similar in spirit to the present version, but
may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by

the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Library General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Library General Public License for more details.

You should have received a copy of the GNU Library General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your

freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price.

Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which
gives you legal permission to copy,
distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively

when run, you must cause it, when started running for such
interactive use in the most ordinary way, to print or display an
announcement including an appropriate copyright notice and a
notice that there is no warranty (or else, saying that you provide
a warranty) and that users may redistribute the program under
these conditions, and telling the user how to view a copy of this
License. (Exception: if the Program itself is interactive but
does not normally print such an announcement, your work based on
the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If
identifiable sections of that work
are not derived from the Program,
and can be reasonably considered independent and separate works in
themselves, then this License, and its terms, do not apply to those
sections when you distribute them as separate works. But when you
distribute the same sections as part of a whole which is a work based
on the Program, the distribution of the whole must be on the terms of
this License, whose permissions for other licensees extend to the
entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest
your rights to work written entirely by you; rather, the intent is to
exercise the right to control the distribution of derivative or
collective works based on the Program.

In addition, mere aggregation of another work not based on the Program
with the Program (or with a work based on the Program) on a volume of
a storage or distribution medium does not bring the other work under
the scope of this License.

3. You may copy and distribute the Program (or a work based on it,
under Section 2) in object code or executable form under the terms of
Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable
source code, which must be distributed under the terms of Sections
1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three
years, to give any third party, for a charge no more than your
cost of physically performing source distribution, a complete
machine-readable copy of the corresponding source code, to be
distributed under the terms of Sections 1 and 2 above on a medium
customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer
to distribute corresponding source code. (This alternative is

allowed only for noncommercial distribution
and only if you
received the program in object code or executable form with such
an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source
code, even though third parties are not
compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing
or modifying
the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing
version number. If the Program
specifies a version number of this License which applies to it and "any
later version", you have the option of following the terms and conditions
either of that version or of any later version published by the Free
Software Foundation. If the Program does not specify a version number of
this License, you may choose any version ever published by the Free Software
Foundation.

10. If you wish to incorporate parts of the Program into other free
programs whose distribution conditions are different, write to the author
to ask for permission. For software which is copyrighted by the Free
Software Foundation, write to the Free Software Foundation; we sometimes
make exceptions for this. Our decision will be guided by the two goals
of preserving the free status of all derivatives of our free software and
of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE,
THERE IS NO WARRANTY
FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES
PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED
OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS
TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE
PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING,
REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING
WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR
REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES,
INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING
OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED
TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY
YOU OR
THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER
PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE
POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest
possible use to the public, the best way to achieve this is to make it
free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest
to attach them to the start of each source file to most effectively
convey the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU
General Public License as published by
the Free Software Foundation; either version 2 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License along
with this program; if not, write to the Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute
it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library,
whether gratis
or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software
patents pose a constant threat to the existence of
any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits
such linking only if the
entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages

are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under

copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into
another language. (Hereinafter, translation is
included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium,
provided that
you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the
terms of this License.

d) If a facility in the modified Library refers to a function or a

table of data to be supplied by an application program that uses
the facility, other than as an argument passed when the facility
is invoked, then you must make a good faith effort to ensure that,
in the event an application does not supply such function or
table, the facility still operates, and performs whatever part of
its purpose remains meaningful.

(For example, a function in a library to compute square roots has
a purpose that is entirely well-defined independent of the
application. Therefore, Subsection 2d requires that any
application-supplied function or table used by this function must
be optional: if the application does not supply it, the square
root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be
reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary
GNU General Public
License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all

subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the

object code for the work under the terms of Section 6.
Any executables containing that work also fall under Section 6,
whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or
link a "work that uses the Library" with the Library to produce a
work containing portions of the Library, and distribute that work
under terms of your choice, provided that the terms permit
modification of the work for the customer's own use and reverse
engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the
Library is used in it and that the Library and its use are covered by
this License. You must supply a copy of this License. If the work
during execution displays copyright notices, you must include the
copyright notice for the Library among them, as well as a reference
directing the user to the copy of this License. Also, you must do one
of these things:

a) Accompany
the work with the complete corresponding
machine-readable source code for the Library including whatever
changes were used in the work (which must be distributed under
Sections 1 and 2 above); and, if the work is an executable linked
with the Library, with the complete machine-readable "work that
uses the Library", as object code and/or source code, so that the
user can modify the Library and then relink to produce a modified
executable containing the modified Library. (It is understood
that the user who changes the contents of definitions files in the
Library will not necessarily be able to recompile the application
to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the
Library. A suitable mechanism is one that (1) uses at run time a
copy of the library already present on the user's computer system,
rather than copying library functions into the executable, and (2)
will operate
properly with a modified version of the library, if
the user installs one, as long as the modified version is
interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at
least three years, to give the same user the materials
specified in Subsection 6a, above, for a charge no more
than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy
from a designated place, offer equivalent access to copy the above

specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally
distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any
other library
facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or

distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in
certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Library under this License may add
an explicit geographical distribution limitation excluding those countries,
so that distribution is permitted only in or among countries not thus
excluded. In such case, this License incorporates the limitation as if
written in the body of this License.

13. The Free Software Foundation may publish
revised and/or new
versions of the Lesser General Public License from time to time.
Such new versions will be similar in spirit to the present version,
but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library
specifies a version number of this License which applies to it and
"any later version", you have the option of following the terms and
conditions either of that version or of any later version published by
the Free Software Foundation. If the Library does not specify a
license version number, you may choose any version ever published by
the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free
programs whose distribution conditions are incompatible with these,
write to the author to ask for permission. For software which is
copyrighted by the Free Software Foundation, write to the Free
Software Foundation; we sometimes make exceptions for this. Our
decision
will be guided by the two goals of preserving the free status
of all derivatives of our free software and of promoting the sharing
and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO
WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW.
EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR
OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY
KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE
LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME
THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN
WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY
AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE,

BE LIABLE TO YOU
FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey
the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the
library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
notice, this list of conditions, and the following disclaimer,
without modification.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.
3. The names of the above-listed copyright holders may not be used
to endorse or promote products derived from this software without
specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT,
INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
X11 License
Copyright (C) 1996 X Consortium

Permission is hereby granted, free of charge, to any person obtaining a copy of
this software and associated documentation files (the "Software"), to deal in
the Software without restriction, including without limitation the rights to
use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies
of the Software, and to permit persons to whom the Software is furnished to do
so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all
copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,

FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE X CONSORTIUM BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE
OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of the X Consortium shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization from the X Consortium.

X Window System is a trademark of X Consortium, Inc.

1.125 mbed-tls TLS 2.6.0

1.125.1 Available under license :

-----BEGIN CERTIFICATE REQUEST-----
MIICnzCCAYcCAQAwPDELMAkGA1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NMMRow
GAYDVQQDExFQb2xhclNTTCBTZXJ2ZXIgMTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAKkCHz1AatVVU4v9Nu6CZS4VYV6Jv7joRZDb7ogWUtPxQ1BHlhJZ
ZIdr/SvgRvlzvt3PkuGRW+1moG+JKXlFgNCDatVBQ3dfOXwJBEeCsFc5cO2j7BUZ
HqgzCEfBBUKp/UzDtN/dBh9NEFFAZ3MTD0D4bYElXwqxU8YwfhU5rPla7n+SnqYF
W+cTl4W1I5LZ1CQG1QkliXUH3aYajz8JGb6tZSxk65Wb3P5BXhem2mxbacwCuhQs
FiScStzN0PdSZ3PxLaAj/X70McotcMqJCwTbLqZPcG6ezr1YieJTWZ5uWpJl4og/
DJQZo93l6J2VE+0p26twEtxaymsXq1KCVLECAwEAAaAeMBwGCSqGSIb3DQEJDjEP
MA0wCwYDVR0PBAQDAgHgMA0GCSqGSIb3DQEBBQUAA4IBAQCj6jCu0wE5OQ1JGQwZ
FNwPqZrvKntSq2yLIbgmGxwlvDLxOzn0KmidSFiKRqh0KXwj9siodlz5C0d9tUqq
7xUXg+j+wDHqUV8zo42Jke+UmWXFPpnXx/fDFGTITdLSn8ZDxkt31ESLTEVZvPFD
odm+C+zWJtKpyL+9op4KvyBQ1MZ9nWZpwMaK4g4mdtOIsz75gMa74w8ZT7VzhGMY
cZGmafsl7x++GDDtf0oCPgrj9xy+Ovv/GyUBaB+6lweflTfPDTRSoN0meFlP5ynF
vqcBM5JKH2FUQIizfc9o6Z8tKxe9FCov3x8szAuoMRA7bjhVngeQIrEkTcaQBvBY
NalC
-----END CERTIFICATE REQUEST-----
-----BEGIN CERTIFICATE-----
MIIBWjCCAQCgAwIBAgIBSzAKBggqhkjOPQQDAjBKMQswCQYDVQQGEwJVSzERMA8G
A1UEChMIbWJlZCBUTFMxKDAmBgNVBAMTH21iZWQgVExTIFRlc3QgaW50ZXJtZWRp
YXRlIENBIDMwHhcNMTUwOTAxMTM0NzU1WhcNMjUwODI5MTM0NzU1WjAUMRIwEAYD
VQQDEwlsb2NhbGhvc3QwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQcbffp2qXq
oZyychmoCRxzrd4Vu96m47NPBehtEC46aTeXgDnBdf++znABrAtfXBRNQz8ARIeY
Bmskr22rlKjyow0wCzAJBgNVHRMEAjAAMAoGCCqGSM49BAMCA0gAMEUCIQDLc+Io
rg8VxEbCgVv8iH+kOIEn9MjhpvKzvwUoV+6rjQIgZU/RXAyc1a+H2+soGfNEIOBQ
AzO3pJx7WJAApZuBX1Q=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIBwjCCAUegAwIBAgIBSTAKBggqhkjOPQQDAjBLMQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxKTAnBgNVBAMTIFBvbGFyU1NMIFRlc3QgSW50ZXJtZWRp
YXRlIEVDIENBMB4XDTE1MDkwMTEzNDIxOFoXDTI1MDgyOTEzNDIxOFowSjELMAkG
A1UEBhMCVUsxETAPBgNVBAoTCG1iZWQgVExTMSgwJgYDVQQDEx9tYmVkIFRMUyBU

ZXN0IGludGVybWVkaWF0ZSBDQSAzMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE
732fWHLNPMPsP1U1ibXvb55erlEVMlpXBGsj+KYwVqU1XCmW9Z9hhP7X/5js/DX9
2J/utoHyjUtVpQOzdTrbsaMdMBswDAYDVR0TBAUwAwEB/zALBgNVHQ8EBAMCB4Aw
CgYIKoZIzj0EAwIDaQAwZgIxAJ9RX38bht+RNsQI2GUpNhC/Y+Tb1OU74O4iEa6+
CkjBWTpLtHRKVdZq7ST0wk1LsQIxAIUi8L1Vx4DuUP0bJxIX/nuJqlBnBG+qRhSf
VgHKgSyHidpZAJpaRi4IkY504CY/Yg==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIC6TCCAdGgAwIBAgIBDzANBgkqhkiG9w0BAQsFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTMwOTI0MTYwODQyWhcNMjMwOTIyMTYwODQyWjBLMQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxKTAnBgNVBAMTIFBvbGFyU1NMIFRlc3QgSW50ZXJtZWRp
YXRlIEVDIENBMHYwEAYHKoZIzj0CAQYFK4EEACIDYgAE8Oih3fX5SLeN1dmFncQl
WMw9+Y6sXblhlrXBxhXxjwdwpCHENn+foUVdrqYVYa7Suv3QVeO6nJ19H3QNixW8
ik1P+hxsbaq8bta78vAyHmC4EmXQLg1w7oxb9Q82qX1Yo4GVMIGSMB0GA1UdDgQW
BBQPib1jQevLXhco/2gwPcGI0JxYOTBjBgNVHSMEXDBagBS0WuSls97SUva51aaV
D+s+vMf9/6E/pD0wOzELMAkGA1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NMMRkw
FwYDVQQDExBQb2xhclNTTCBUZXN0IENBggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZI
hvcNAQELBQADggEBAAjeaTUaCBiXT1CYLVr6UFSeRNZBrDPnj6PwqUQTvgB5I5n6
yXqoE4RYDaEL0Lg24juFxI26itBuypto6vscgGq77cfrP/avSdxU+xeZ4bCWvh3M
ddj9lmko2U8I8GhBcHpSuIiTvgKDB8eKkjeq3AsLGchHDvip8pB3IhcNfL7W94Zf
7/lH9VQiE3/px7amD32cidoPvWLA9U3f1FsPmJESUz0wwNfINpDjmPr8dGbkCN+M
CFhxo6sCfK8KLYG4nYX8FwxVR86kpSrO9e84AX0YYbdzxprbc2XOaebJ8+BDmzut
ARkD7DTXrodN1wV7jQJkrUuEwPj9Rhvk+MFRkaw=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIBWjCCAQCgAwIBAgIBSzAKBggqhkjOPQQDAjBKMQswCQYDVQQGEwJVSzERMA8G
A1UEChMIbWJlZCBUTFMxKDAmBgNVBAMTH21iZWQgVExTIFRlc3QgaW50ZXJtZWRp
YXRlIENBIDMwHhcNMTUwOTAxMTM0NzU1WhcNMjUwODI5MTM0NzU1WjAUMRIwEAYD
VQQDEwlsb2NhbGhvc3QwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQcbffp2qXq
oZyychmoCRxzrd4Vu96m47NPBehtEC46aTeXgDnBdf++znABrAtfXBRNQz8ARIeY
Bmskr22rlKjyow0wCzAJBgNVHRMEAjAAMAoGCCqGSM49BAMCA0gAMEUCIQDLc+Io
rg8VxEbCgVv8iH+kOIEn9MjhpvKzvwUoV+6rjQIgZU/RXAyc1a+H2+soGfNEIOBQ
AzO3pJx7WJAApZuBX1Q=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIBtDCCATqgAwIBAgIBTTAKBggqhkjOPQQDAjBLMQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxKTAnBgNVBAMTIFBvbGFyU1NMIFRlc3QgSW50ZXJtZWRp
YXRlIEVDIENBMB4XDTE1MDkwMTE0MDg0M1oXDTI1MDgyOTE0MDg0M1owSjELMAkG
A1UEBhMCVUsxETAPBgNVBAoTCG1iZWQgVExTMSgwJgYDVQQDEx9tYmVkIFRMUyBU
ZXN0IGludGVybWVkaWF0ZSBDQSAzMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE
732fWHLNPMPsP1U1ibXvb55erlEVMlpXBGsj+KYwVqU1XCmW9Z9hhP7X/5js/DX9
2J/utoHyjUtVpQOzdTrbsaMQMA4wDAYDVR0TBAUwAwEB/zAKBggqhkjOPQQDAgNo
ADBlAjAJRxbGRas3NBmk9MnGWXg7PT1xnRELHRWWIvfLdVQt06l1/xFg3ZuPdQdt
Qh7CK80CMQD7wa1o1a8qyDKBfLN636uKmKGga0E+vYXBeFCy9oARBangGCB0B2vt
pz590JvGWfM=

-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIC6TCCAdGgAwIBAgIBDzANBgkqhkiG9w0BAQsFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTMwOTI0MTYwODQyWhcNMjMwOTIyMTYwODQyWjBLMQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxKTAnBgNVBAMTIFBvbGFyU1NMIFRlc3QgSW50ZXJtZWRp
YXRlIEVDIENBMHYwEAYHKoZIzj0CAQYFK4EEACIDYgAE8Oih3fX5SLeN1dmFncQl
WMw9+Y6sXblhlrXBxhXxjwdwpCHENn+foUVdrqYVYa7Suv3QVeO6nJ19H3QNixW8
ik1P+hxsbaq8bta78vAyHmC4EmXQLg1w7oxb9Q82qX1Yo4GVMIGSMB0GA1UdDgQW
BBQPib1jQevLXhco/2gwPcGI0JxYOTBjBgNVHSMEXDBagBS0WuSls97SUva51aaV
D+s+vMf9/6E/pD0wOzELMAkGA1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NMMRkw
FwYDVQQDExBQb2xhclNTTCBUZXN0IENBggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZI
hvcNAQELBQADggEBAAjeaTUaCBiXT1CYLVr6UFSeRNZBrDPnj6PwqUQTvgB5I5n6
yXqoE4RYDaEL0Lg24juFxI26itBuypto6vscgGq77cfrP/avSdxU+xeZ4bCWvh3M
ddj9lmko2U8I8GhBcHpSuIiTvgKDB8eKkjeq3AsLGchHDvip8pB3IhcNfL7W94Zf
7/lH9VQiE3/px7amD32cidoPvWLA9U3f1FsPmJESUz0wwNfINpDjmPr8dGbkCN+M
CFhxo6sCfK8KLYG4nYX8FwxVR86kpSrO9e84AX0YYbdzxprbc2XOaebJ8+BDmzut
ARkD7DTXrodN1wV7jQJkrUuEwPj9Rhvk+MFRkaw=
-----END
CERTIFICATE-----
00 0
*H=0>10 UNL10U
PolarSSL10UPolarssl Test EC CA0
130924155204Z
230922155204Z0410 UNL10U
PolarSSL10U localhost0Y0*H=*H=B7Vv Zr>Y- n|th"YbN#/4]]kw
U*00 U00UPaecF0nU#g0em $I?+x~$6|B@0>10 UNL10U
PolarSSL10UPolarssl Test EC CA C~bC0
*H=h0e1,\d
Na1ssT]/!)5>90!6]'%;5%Y^|f{Os!R*'&z
-----BEGIN X509 CRL-----
MIIBqzCBlDANBgkqhkiG9w0BAQIFADA7MQswCQYDVQQGEwJOTDERMA8GA1UEChMI
UG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EXDTA5MDcxOTE5NTYz
N1oXDTA5MDkxNzE5NTYzN1owKDASAgEBFw0wOTAyMDkyMTEyMzZaMBICAQMXDTA5
MDIwOTIxMTIzNlowDQYJKoZIhvcNAQECBQADggEBAF8F5y82zgtxcwQ4aFvrkanT
ygyd5+RW/Y//vpck44V+CYx1d1r+QkauaXel9qUKBPsg2dUwQ+jwV/m+Sp2MHaX5
NfW7XUb7Ji4yhwgh9/9vFPqqnKBf9esLJuJoQ4mLhcGB5J1yCcavLrynvB4PJEnG
graTbbyizelXBmk3ApvNYxczJZxt7EzpVbrFaev7myGmOffdDkIMc2WDpDkyLTlU
kITjB7fMJhD/dgNskKZ4fgkKKKPCMJrJPO67Wzwqx/6vsrZcACB9X+143WZr4GVO
Fw2SaMnqfVLlUEndoOpbLCU4ugcc82kQQF3TsovXJYW7XqoWl2u/ENCwShl9rl4=
-----END X509 CRL-----
-----BEGIN X509 CRL-----
MIIBgzCCAQoCAQEwCQYHKoZIzj0EATA+MQswCQYDVQQGEwJOTDERMA8GA1UEChMI
UG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EXDTMyMDMxMDEx
MDUxNVoXDTQyMDMwODExMDUxNVowKDASAgEKFw0xMzA5MjQxNjI4MzhaMBICARYX
DTE0MDEyMDEzNDMwNVqgcjBwMG4GA1UdIwRnMGWAFJ1tICRJAT8ry3i1Gbx+JMnb
+zZ8oUKkQDA+MQswCQYDVQQGEwJOTDERMA8GA1UEChMIUG9sYXJTU0wxHDAaBgNV

BAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0GCCQDBQ+J+YkPM6DAJBgcqhkjOPQQBA2gA
MGUCMQCmsvNsOQdbGpmzpeZlKU9lDP6yyWenrI/89swZYogE3cSPob4tOzeYg38i
or91IPgCMD7N/0Qz6Nq2IgBtZORLgsA0ltK+W6AOS+/EIhvGuXV8uguUyYknl4vb
+cE+lWxhCQ==
-----END X509 CRL-----
-----BEGIN X509 CRL-----
MIIBqzCBlDANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDERMA8GA1UEChMI
UG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EXDTExMDIyMDEwMjI1
OVoXDTE5MTEyNTEwMjI1OVowKDASAgEBFw0xMTAyMTIxNDQ0MDdaMBICAQMXDTEx
MDIxMjE0NDQwN1owDQYJKoZIhvcNAQEFBQADggEBAJYuWdKPdblMVWCnxpMnchuL
dqWzK2BA0RelCaGjpxuwX3NmLDm+5hKja/DJxaRqTOf4RSC3kcX8CdIldsLO96dz
//wAQdFPDhy6AFT5vKTO8ItPHDb7qFOqFqpeJi5XN1yoZGTB1ei0mgD3xBaKbp6U
yCOZJSIFomt7piT4GcgWVHLUmpyHDDeodNhYPrN0jf2mr+ECd9fQJYdz1qm0Xx+Q
NbKXDiPRmPX0qVleCZSeSp1JAmU4GoCO+96qQUpjgll+6xWya3UNj61f9sh0Zzr7
5ug2LZo5uBM/LpNR1K3TLxNCcg7uUPTn9r143d7ivJhPl3tEJn4PXjv6mlLoOgU=
-----END
X509 CRL-----
-----BEGIN EC PARAMETERS-----
BggqhkjOPQMBBw==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIL1c0zvh4Fx8aylrlHsOsK5Pcam7BWVHM2lDxGO26QIUoAoGCCqGSM49
AwEHoUQDQgAEJSlIjKErLP4bE2rHnanQdgQjhiYU7dIYFBnlJ1jWdbLzuMp9BpBR
2dPPvn5djCqo6Y/lV6tCUhRchlDoJoItxw==
-----END EC PRIVATE KEY-----
-----BEGIN X509 CRL-----
MIIBqzCBlDANBgkqhkiG9w0BAQwFADA7MQswCQYDVQQGEwJOTDERMA8GA1UEChMI
UG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EXDTExMDIxMjE0NDQw
N1oXDTExMDQxMzE0NDQwN1owKDASAgEBFw0xMTAyMTIxNDQ0MDdaMBICAQMXDTEx
MDIxMjE0NDQwN1owDQYJKoZIhvcNAQEMBQADggEBAC0GpmRvsrvshp1q/SXk80HA
m28ZvEuys9zY5/AnrtYHQfsX9QRJk5li7PlnzHtVGp8I5Qi4mJVPaJ+JmhqAc/oo
NPmxDx8m9XF9v0XHzqQZIWlPXH8QM9WLzTazbQFXhuwnZ6LPhpo+m8cbN91mUFil
9g+SGkma+VYV+yPRNmKyldcRVvPZUIkhTCMWkZoYrbDXUmkVQpsgz2c5ksIeMI/7
4Qj9J38I9AOt0DlQ3etFhNc0OMnR7zY8tn9B4dejoNklEZfiyDxsDZVPusZrxnWM
WxuehOGHZf3YESjLMtR7BW26QRHIF/nhGDHsbLiunxXI6eJlbYFoZMfwc6TMqnc=
-----END X509 CRL-----
-----BEGIN CERTIFICATE-----
MIIEATCCAumgAwIBAgIBAjANBgkqhkiG9w0BAQUFADBxMRMwEQYDVQQDDApUZXN0
IENBIDAxMREwDwYDVQQIDAhFY25pdm9ycDELMAkGA1UEBhMCWFgxHjAcBgkqhkiG
9w0BCQEWD3RjYUBleGFtcGxlLmNvbTEaMBgGA1UECgwRVGVzdCBDQSBBdXRob3Jp
dHkwHhcNMTUwMzExMTIwNjUxWhcNMjUwMzA4MTIwNjUxWjCBmzELMAkGA1UEBhMC
WFgxDDAKBgNVBAoMA3RjYTERMA8GA1UECAwIRWNuaXZvcnAxDDAKBgNVBAsMA1RD
QTEPMA0GA1UEAwwGQ2xpZW50MSEwHwYJKoZIhvcNAQkBFhJjbGllbnRAZXhhbXBs
ZS5jb20xEzARBgNVBAUTCjcxMDEwMTIyNTUxFDASBgNVBC0DCwA3MTAxMDEyMjU1
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnQS0JLb8Dqy8V2mszkWk
V8c/NPQcG3ivueXZHqOT9JTiPqrigGcLHtlmlaJ0aUUxix7q60aOds041TFyeknT
SUFYY4ppOhiP+fOpWKPv4ZMwhSI2XzcgYhQSNHV0lIG1we9RAAfumomDMq7oMJhb
EGf0ihibbwZXPUwBlm10GaB4K93PNY8Bz4ekBxzQ1WJkQ5LGsQnVZSuLnvp5dWSe

J2axxyY4hPXR30jzEyZvy4kv4nzAu5lqZ5XKLrRO4TKwZrtr+CCPVkPJRE36rWYt
tQaJEEpNOo0ZPpTtG6F8/tGh5r8jFx/f6wG+nyANJJ98kEP8i6TPjRrg+697mLcd
iQIDAQABo3kwdzAJBgNVHRMEAjAAMDYGA1UdHwQvMC0wK6ApoCeGJWh0dHA6Ly9j
cmwuZXhhbXBsZS5jb20vdGVzdF9jYV8wMS5jcmwwEwYDVR0lBAwwCgYIKwYBBQUH
AwIwHQYDVR0RBBYwFIESY2xpZW50QGV4YW1wbGUuY29tMA0GCSqGSIb3DQEBBQUA
A4IBAQBySELCnU8/PtGIG3dwhJENOSU5R7w8jpRXxHCuSBR+W6nuUCISz+z+EdF/
A7AOJDASuS+4gkrSSmQhGFpf7E5VbF8trVZhLAZrXqKMcUreKH6v0I8MAUXmIs3G
tqiBGf7pSYJN9DvVOOgANjdy6THuUzYv5qSvBZ4pNYEfHSlMNrV7niynd8dgPOML
pA7GUfv5k2mMkMbSD15pTMgcavrBKYgyqcvF1C3qghfoL5+i38H8sKzF8hy7wHtE
ESHtBq20RYA3m0UcA0e64GcanO2Ps/AQVBc7qMeHbqnqj3uUhtTkQcMUWnMgy1NR
5RbzoLMOxq7hoOCyIaQeM/wgxeGE
-----END
CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAnQS0JLb8Dqy8V2mszkWkV8c/NPQcG3ivueXZHqOT9JTiPqri
gGcLHtlmlaJ0aUUxix7q60aOds041TFyeknTSUFYY4ppOhiP+fOpWKPv4ZMwhSI2
XzcgYhQSNHV0lIG1we9RAAfumomDMq7oMJhbEGf0ihibbwZXPUwBlm10GaB4K93P
NY8Bz4ekBxzQ1WJkQ5LGsQnVZSuLnvp5dWSeJ2axxyY4hPXR30jzEyZvy4kv4nzA
u5lqZ5XKLrRO4TKwZrtr+CCPVkPJRE36rWYttQaJEEpNOo0ZPpTtG6F8/tGh5r8j
Fx/f6wG+nyANJJ98kEP8i6TPjRrg+697mLcdiQIDAQABAoIBAF7i3MnjGmbz080v
OxJb23iAG54wdlvTjr3UPGTbjSmcXyxnsADQRFQcJHYAekCzY8EiqewL80OvuMx8
2SU1P81hA70Dg5tsBHWT3Z6HUwsKG6QYjKr1cUhTwLyazhyAVgogSN6v7GzO9M3I
DOBw8Xb0mz5oqGVre4S7TapN8n8ZG5oWm0XKGACXy0KbzY0KvWdkUzumFQ8X/ARE
FsWyu+O69EbMqZRUKu45SrcubsdVGjOwseZHkmp5V6pc6Q/OrTHZqXJtDva5UIRq
+Lof5scy9jiwwRnM/klvh23mz0ySU4YA3645m5KqyWR4YJCR1MnMANmXUSeYWfYz
19+R1gECgYEAzm83lI7eIhTH38H0/jFpf3R7vNjPX3TR5waa4EXsCxhTOpoL89mR
iNmzH0aOC4OR8rz/9PCnwmtH1lyQ4r/RokBmCp3pBxeWSlenFfV3rLCeEDo0Q/OL
SX5DL4IbZD0VmNDt606WS7AEv93GhpN03Anw6kgHQUm1l030PR9DYZECgYEAwrgO
/RyB/Ehw7smlysZb2sn1lvd6z8fg+pcu8ZNRKODaYCCOb8p1lnHrnIQdEmjhlmVp
HAEuJ5jxCb+lyruV+dlx+0W/p6lHtKr0iBHG8EFkHnjN6Y+59Qu0HfSm0pZw7Ftr
QcUDPuDJkTVUAvrZqciWlwzTWCC9KYXtasT+AHkCgYEAnP80dAUbpyvKvr/RxShr
JYW/PWZegChmIp+BViOXWvDLC3xwrqm+5yc59QVBrjwH2WYn+26zB0dzwPFxNyHP
GuiDMnvZ54zmve9foXGn7Gv+KjU53pvwSJqAGjeHAXr7W9c5uoVwBGv/kLPn8h1e
+KGO2X6iFeMq+cFNiNan9iECgYBj+oGnsKWFVeS2ls8LyMGNGzmAZF2opiZ8RHgU
DeIULS+zP8Qi3j92GdQyLxuGQlfiEvvfJzP9nOfWa5LC/4JIIUAHFo8LlT1+JHEe
FJKi9dBkXP7NN8DxcyruXpnxctFUarQttuytslmMt2cFiKuOI7I+qJUzoMu/sEZx
FeidcQKBgQCuralmtbl4nxjn3aR/ZgFTAKCL9WaJPh5hFJ9q4UuWxJdBX5z3Ey3/
70ehLKYPumjmZtXynzz4BTWj1W9X+tgj/499uzV6LdQERGjT6WVy8xR9RELWW0an
N9N1IAc4qTSjbI4EIMwMBSAoFfCux/jfDkG4g+RDnpV92sqxz2CtKg==
-----END
RSA PRIVATE KEY-----
ECDH primitive random #1
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
ecdh_primitive_random:MBEDTLS_ECP_DP_SECP192R1

ECDH primitive random #2
depends_on:MBEDTLS_ECP_DP_SECP224R1_ENABLED
ecdh_primitive_random:MBEDTLS_ECP_DP_SECP224R1

ECDH primitive random #3
depends_on:MBEDTLS_ECP_DP_SECP256R1_ENABLED
ecdh_primitive_random:MBEDTLS_ECP_DP_SECP256R1

ECDH primitive random #4
depends_on:MBEDTLS_ECP_DP_SECP384R1_ENABLED
ecdh_primitive_random:MBEDTLS_ECP_DP_SECP384R1

ECDH primitive random #5
depends_on:MBEDTLS_ECP_DP_SECP521R1_ENABLED
ecdh_primitive_random:MBEDTLS_ECP_DP_SECP521R1

ECDH primitive rfc 5903 p256
depends_on:MBEDTLS_ECP_DP_SECP256R1_ENABLED
ecdh_primitive_testvec:MBEDTLS_ECP_DP_SECP256R1:"C88F01F510D9AC3F70A292DAA2316DE544E9AA
B8AFE84049C62A9C57862D1433":"DAD0B65394221CF9B051E1FECA5787D098DFE637FC90B9EF945D0C3
772581180":"5271A0461CDB8252D61F1C456FA3E59AB1F45B33ACCF5F58389E0577B8990BB3":"C6EF9C5
D78AE012A011164ACB397CE2088685D8F06BF9BE0B283AB46476BEE53":"D12DFB5289C8D4F81208B7027
0398C342296970A0BCCB74C736FC7554494BF63":"56FBF3CA366CC23E8157854C13C58D6AAC23F046ADA
30F8353E74F33039872AB":"D6840F6B42F6EDAFD13116E0E12565202FEF8E9ECE7DCE03812464D04B9442
DE"

ECDH
primitive rfc 5903 p384
depends_on:MBEDTLS_ECP_DP_SECP384R1_ENABLED
ecdh_primitive_testvec:MBEDTLS_ECP_DP_SECP384R1:"099F3C7034D4A2C699884D73A375A67F7624EF7C
6B3C0F160647B67414DCE655E35B538041E649EE3FAEF896783AB194":"667842D7D180AC2CDE6F74F3755
1F55755C7645C20EF73E31634FE72B4C55EE6DE3AC808ACB4BDB4C88732AEE95F41AA":"9482ED1FC0EE
B9CAFC4984625CCFC23F65032149E0E144ADA024181535A0F38EEB9FCFF3C2C947DAE69B4C634573A81
C":"41CB0779B4BDB85D47846725FBEC3C9430FAB46CC8DC5060855CC9BDA0AA2942E0308312916B8ED
2960E4BD55A7448FC":"E558DBEF53EECDE3D3FCCFC1AEA08A89A987475D12FD950D83CFA41732BC509
D0D1AC43A0336DEF96FDA41D0774A3571":"DCFBEC7AACF3196472169E838430367F66EEBE3C6E70C416
DD5F0C68759DD1FFF83FA40142209DFF5EAAD96DB9E6386C":"11187331C279962D93D604243FD592CB9
D0A926F422E47187521287E7156C5C4D603135569B9E9D09CF5D4A270F59746"

ECDH primitive
rfc 5903 p521
depends_on:MBEDTLS_ECP_DP_SECP521R1_ENABLED
ecdh_primitive_testvec:MBEDTLS_ECP_DP_SECP521R1:"0037ADE9319A89F4DABDB3EF411AACCCA5123
C61ACAB57B5393DCE47608172A095AA85A30FE1C2952C6771D937BA9777F5957B2639BAB072462F68C27
A57382D4A52":"0015417E84DBF28C0AD3C278713349DC7DF153C897A1891BD98BAB4357C9ECBEE1E3BF
42E00B8E380AEAE57C2D107564941885942AF5A7F4601723C4195D176CED3E":"017CAE20B6641D2EEB69
5786D8C946146239D099E18E1D5A514C739D7CB4A10AD8A788015AC405D7799DC75E7B7D5B6CF2261A6
A7F1507438BF01BEB6CA3926F9582":"0145BA99A847AF43793FDD0E872E7CDFA16BE30FDC780F97BCCC
3F078380201E9C677D600B343757A3BDBF2A3163E4C2F869CCA7458AA4A4EFFC311F5CB151685EB9":"00
D0B3975AC4B799F5BEA16D5E13E9AF971D5E9B984C9F39728B5E5739735A219B97C356436ADC6E95BB0
352F6BE64A6C2912D4EF2D0433CED2B6171640012D9460F":"015C68226383956E3BD066E797B623C27CE0

EAC2F551A10C2C724D9852077B87220B6536C5C408A1D2AEBB8E86D678AE49CB57091F4732296579AB44
FCD17F0FC56A":"01144C7D79AE6956BC8EDB8E7C787C4521CB086FA64407F97894E5E6B2D79B04D1427
E73CA4BAA240A34786859810C06B3C715A3A8CC3151F2BEE417996D19F3DDEA"

ECDH
exchange #1
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
ecdh_exchange:MBEDTLS_ECP_DP_SECP192R1

ECDH exchange #2
depends_on:MBEDTLS_ECP_DP_SECP521R1_ENABLED
ecdh_exchange:MBEDTLS_ECP_DP_SECP521R1
-----BEGIN CERTIFICATE-----
MIIDBzCCAe+gAwIBAgIBATANBgkqhkiG9w0BAQsFADAWMRQwEgYDVQQDEwtUZXN0
IHJvb3QgMjAeFw0wMTAxMDEwMDAwMDBaFw0zMDEyMzEyMzU5NTlaMCYxJDAiBgNV
BAMTG1Rlc3QgaW50ZXJtZWRpYXRlIG1heHBhdGggMTCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBANpGlBMXdo8cO9oqUw/b6PMwiMNV8LCe6wB9VKHPa6OG
Q0o8Xqktgwnh1rojgpMhbCApE7UXeMr6ZGq/NtqmO1hO5adV5JehWZyvg7j4EBpG
g8iWo0jNpKMJ0Yx1uBkkljEdZLTHa4bK/zy2NKqDNS2yWs9/M5+xw5XE2ecAg7FT
cXhf3q50V+M6T2IaQ9BxntTyCT8IIF2eRM/t9Y944s9Rfzm/KQVKRYPudX7YhTt9
iqCJB4JoqYhs3HEO0wPkJxY4KBTUCN94s+7jUFdRrYxe+8Ya6tIYWqD38i5qdGhY
xrVey1LatsDJQ2EgNYobM/LjoCLK1WUssEqf0OU2bi0CAwEAAaNQME4wDAYDVR0T
BAUwAwEBATAdBgNVHQ4EFgQUOBl8edVm/H5xdS2EGEeLzftZ/DUwHwYDVR0jBBgw
FoAUjgXdXx9NGPa+UvHBC4//SE+ARpQwDQYJKoZIhvcNAQELBQADggEBAFwZriTu
DKkiDHFfz3UX4fIxYTHCi4TveYZGPeTbxhBb3XZC5qDF4T5HvCTSkG9+oFfZzI1a
lPN2yZB7QnmHJoyWa5fuovwUL0iI3iIZMqU56tdVPW8gkJe++U5kHMSpz2VF0eo8
7XkKWxZovRwczgfDFRP9zM9CylyzQjqxx6kbxJozWnwc5UrVbJMaPIqonXp1nDoZ
i878+hX4rJUEjgO6Sa9GVZQpmuCrQF0qKsTiUBzZN67hoD3xoTAYi5IXQE2tRD1N
j3zwng9liCsxurGMnuV0BPWv/IDYRu/syjee1Qv1VFeRto5D4Rldmi2p1f5iWJCk
5m5YpRsknaICjYs=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDDDCCAfSgAwIBAgIBATANBgkqhkiG9w0BAQsFADAmMSQwIgYDVQQDExtUZXN0
IGludGVybWVkaWF0ZSBtYXhwYXRoIDEwHhcNMDEwMTAxMDAwMDAwWhcNMzAxMjMx
MjM1OTU5WjAeMRwwGgYDVQQDExNUZXN0IGxlYWYgaW52YWxpZCAyMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAigGgHGNWNkEWWFn7eaU4kC2WjR3RtcBs
oW1MlQndUvwWUHgcbfIg7nh66Oi6Xl3IqAMjHj1J0EPGcwTfmLdaRvN38KjTMh3/
FiFrrUL0MNgiGxjkTthWgsfV4C/i3vRDTCW+2UMFdd6+z7hwFf+ldTsCP9Qp+93G
drslrvAR2W0qjHLULAJGk/6WzxFG6xeCgdhkooDPprsflZJ/cN1SuqTYOaVMAj9J
aovStUTVhF8ouDULpq0fiBImoldObcGdaAWlgRl0k8NdoSLpWd/7+hi4sH5PSOZq
+8g1lQ3cgrE7ta4X3p/i6eApcn1hyEkTy9ZpKOFvZXnM4D1j8+KSKQIDAQABo00w
SzAJBgNVHRMEAjAAMB0GA1UdDgQWBBTCN2vDLY1tcenTzyRmlS4TBe2xijAfBgNV
HSMEGDAWgBQ4GXx51Wb8fnF1LYQYR4vN+1n8NTANBgkqhkiG9w0BAQsFAAOCAQEA
eb/tgtSbrz7j7HQaxGgI5LVedRro3a2fNLhO0wNboGI6gACIPait1ePkUwuMfLfl
Fky2/2VZ8Ie4pQqxFmdSUqf1NSmxgiWLRho4oTiFv1z08LYQgSdKT49ffKO67TDG
D1nI8rEuT1Nupq8WI5jcKgWqktMJjgKzfN+9nCgFGQMGqTBnt7uYZHhnuZfKSJPv
gHmS4gj72OQ2Nu6xORGhd6J8VjzcG6BX1pLebNQRzlHT3E5IVNF/9cCrc+E87Wns

bDGtzhyx7SIP7/2TiJeBZs7p8xXpaDF2cNx2F+jZH+P8feT7c+JoY7A72uVDSlYf
WVf02pylKRgqayOujH3PWA==
-----END
 CERTIFICATE-----
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

aaaa

Z0jkz/tqJOI0vRSdLBbipHnWouyBQ4e/A1yIJdlBtqXxJ1KE/ituHRbNc4j4kL8Z
/r6pvwnTI0PSx2Eqs048YdS92LT6qAv4flbNDxMn2uY7s4ycS4Q8w1JXnCeaAnYm
WYI5wxO+bvRELR2Mcz5DmVnL8jRyml6l6582bSv5oufReFIbyPZbQWlXgYnpu6He
GTc7E1zKYQGG/9+DQUl/1vQuCPqQwny0tQoX2w5tdYpdMdVm+zkLtbajzdTviJJa
TWzL6lt5AoGBAN86+SVeJDcmQJcv4Eq6UhtRr4QGMiQMz0Sod6ettYxYzMgxtw28
CIrgpozCc+UaZJLo7UxvC6an85r1b2nKPCLQFaggJ0H4Q0J/sZOhBIXaoBzWxveK
nupceKdVxGsFi8CDy86DBfiyFivfBj+47BbaQzPBj7C4rK7UlLjab2rDAoGBAN2u
AM2gchoFiu4v1HFL8D7lweEpi6ZnMJjnEu/dEgGQJFjwdpLnPbsj4c75odQ4Gz8g
sw9lao9VVzbusoRE/JGI4aTdO0pATXyG7eG1Qu+5Yc1YGXcCrliA2xM9xx+d7f+s
mPzN+WIEg5GJDYZDjAzHG5BNvi/FfM1C9dOtjv2dAoGAF0t5KmwbjWHBhcVqO4Ic
BVvN3BIlc1ue2YRXEDlxY5b0r8N4XceMgKmW18OHApZxfl8uPDauWZLXOgl4uepv
whZC3EuWrSyyICNhLY21Ah7hbIEBPF3L3ZsOwC+UErL+dXWLdB56Jgy3gZaBeW7b
vDrEnocJbqCm7IukhXHOBK8CgYEAwqdHB0hqyNSzIOGY7v9abzB6pUdA3BZiQvEs
3LjHVd4HPJ2x0N8CgrBIWOE0q8+0hSMmeE96WW/7jD3fPWwCR5zlXknxBQsfv0gP
3BC5PR0Qdypz+d+9zfMf625kyit4T/hzwhDveZUzHnk1Cf+IG7Q+TOEnLnWAWBED
ISOWmrUCgYAFEmRxgwAc/u+D6t0syCwAYh6POtscq9Y0i9GyWk89NzgC4NdwwbBH
4AgahOxIxXx2gxJnq3yfkJfIjwf0s2DyP0kY2y6Ua1OeomPeY9mrIS4tCuDQ6LrE
TB6l9VGoxJL4fyHnZb8L5gGvnB1bbD8cL6YPaDiOhcRseC9vBiEuVg==
-----END
RSA PRIVATE KEY-----
00
*H
0as6DXtvM~I,\`6Dod+xGOfeyk3bI <ht+5/P?-o%qy<<Ea_`SHQ
nB4`=; Yx\ngg 0hUQ)V!AP]sP\.XPVwj c?/HMR;-Vhb_
i{Ql+k.F7^ofb57
wws3<"_09"Tk7L19A@2@LhSIE
)u00n'|RhEml,m&e4K2}T7?c'1
30;?KC9l&RA|Lt0B^{^-J*{^
7#HW=1ng=z~MJCRTzGWq?-7=,\vp4`\K B=X9P}4
}lv5R5P~4I3_a*KuCH~8@-BXZj})i{g/8(X2_oH -Z2o8|<o$p5WBZx}eYpXuz0
6Mn@N_Ccd q C% dv>d~!SSq3LJyiD!-ZmI"KSR/|'c/?WvL2Xg~z7q]IJV"6xIxr'N]s2W[H6Yr
Zj(IHPE5u$J~B!P{C }^-)"i-Nqb=}t~1skr7H`T@ATM}PJWJxZB3nc]S)&IlS]Iuiy09'^DD;erZ[cO%,Q x$e3O`3
=.x`TDi@&P<,"9BOCc)$
-----BEGIN CERTIFICATE-----
MIICIDCCAaWgAwIBAgIBCjAKBggqhkjOPQQDAjA+MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EwHhcN
MTMwOTI0MTU1MjA0WhcNMjMwOTIyMTU1MjA0WjA0MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxEjAQBgNVBAMTCWxvY2FsaG9zdDBZMBMGByqGSM49AgEG
CCqGSM49AwEHA0IABIFZMXZJJPoVraugMW4O7TMR+pElVcGwwZwDcj6Yui2kcjeJ
H0M3jR+OOtjwV+gvT8kApPfbcw+yxgSU0UA7OOOjgZ0wgZowCQYDVR0TBAIwADAd
BgNVHQ4EFgQUfmWPPjMDFOXhvmCy4IV/jOdgK3swbgYDVR0jBGcwZYAUnW0gJEkB
PyvLeLUZvH4kydv7NnyhQqRAMD4xCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQb2xh
clNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBFQyBDQYIJAMFD4n5iQ8zoMAoG
CCqGSM49BAMCA2kAMGYCMQCsYTyleBFuI4nizuxo/ie5dxJnD0ynwCnRJ+84PZP4
AQA3HdUz0qNYs4CZ2am9Gz0CMQDr2TNLFA3C3S3pmgXMT0eKzR1Ca1/Nulf0llQZ
Xj09kLboxuemP40IIqhQnpYptMg=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----

MIIB+zCCAYCgAwIBAgIBATAMBggqhkjOPQQDAgUAMD4xCzAJBgNVBAYTAk5MMREw
DwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBFQyBDQTAe
Fw0yMzA5MjIxNTQ5NDlaFw0zMDEyMzEyMzU5NTlaMD4xCzAJBgNVBAYTAk5MMREw
DwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBFQyBDQTB2
MBAGByqGSM49AgEGBSuBBAAiA2IABMPaKzRBN1gvh1b+/Im6KUNLTuBuww5XUzM5
WNRStJGVOQsj318XJGJI/BqVKc4sLYfCiFKAr9ZqqyHduNMcbli4yuiyaY7zQa0p
w7RfdadHb9UZKVVpmlM7ILRmFmAzHqNQME4wDAYDVR0TBAUwAwEB/zAdBgNVHQ4E
FgQUnW0gJEkBPyvLeLUZvH4kydv7NnwwHwYDVR0jBBgwFoAUnW0gJEkBPyvLeLUZ
vH4kydv7NnwwDAYIKoZIzj0EAwIFAANnADBkAjB1ZNdOM7KRJiPo45hP17A1sJSH
qHFPEJbml6KdNevoVZ1HqvP8AoFGcPJRpQVtzC0CMDa7JEqn0dOss8EmW9pVF/N2
+XvzNczj89mWMgPhJJlT+MONQx3LFQO+TMSI9hLdkw==
-----END
CERTIFICATE-----
-----BEGIN EC PARAMETERS-----
BggqhkjOPQMBBw==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIC9zTt8jgjBlbq+qCsGj6uclaKLYBqxYSmUiuBdM1KG9oAoGCCqGSM49
AwEHoUQDQgAE732fWHLNPMPsP1U1ibXvb55erlEVMlpXBGsj+KYwVqU1XCmW9Z9h
hP7X/5js/DX92J/utoHyjUtVpQOzdTrbsQ==
-----END EC PRIVATE KEY-----
-----BEGIN CERTIFICATE REQUEST-----
MIICsjCCAZoCAQAwPDELMAkGA1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NMMRow
GAYDVQQDExFQb2xhclNTTCBTZXJ2ZXIgMTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAKkCHz1AatVVU4v9Nu6CZS4VYV6Jv7joRZDb7ogWUtPxQ1BHlhJZ
ZIdr/SvgRvlzvt3PkuGRW+1moG+JKXlFgNCDatVBQ3dfOXwJBEeCsFc5cO2j7BUZ
HqgzCEfBBUKp/UzDtN/dBh9NEFFAZ3MTD0D4bYElXwqxU8YwfhU5rPla7n+SnqYF
W+cTl4W1I5LZ1CQG1QkliXUH3aYajz8JGb6tZSxk65Wb3P5BXhem2mxbacwCuhQs
FiScStzN0PdSZ3PxLaAj/X70McotcMqJCwTbLqZPcG6ezr1YieJTWZ5uWpJl4og/
DJQZo93l6J2VE+0p26twEtxaymsXq1KCVLECAwEAAaAxMC8GCSqGSIb3DQEJDjEi
MCAwCwYDVR0PBAQDAgHgMBEGCWCGSAGG+EIBAQQEAwIAQDANBgkqhkiG9w0BAQUF
AAOCAQEANlNG9hW852OzVKj2Z8TtU9jxstAoSCH9yc9Coj4Vw2TTjs1zcuBWsMl1
2bf2I6ZvEH6ZhcQY7i7nyHQyPlqE4l6U9D8ct967QN7smuAHNY2HiQ2++eCBTHck
PdtGJAzIvNlXcoqNi8UC5fGepNtI1usNo41SKMvbg6nGA5gdcQKk7CVlk8lrD0qI
Xn/HvjSRoDE4ZGxAtNvPXWorGSxtgcy8EMPoXVUab5fNt8q//x/NQ4yEQKPrexmR
IuOiQ8VW8QZtkORGpZbGSvskU0WfKANui4zCcXYRc4mVR4Wf0C+fyHeihhjslSnT
RbC7nQn5HSHp31qJlr80QodywaK1Dg==
-----END CERTIFICATE REQUEST-----
Note: This is just a template, so feel free to use/remove the unnecessary things

Description
- Type: Bug | Enhancement\Feature Request | Question
- Priority: Blocker | Major | Minor

Bug

OS

mbed-OS|linux|windows|

mbed TLS build:
Version: x.x.x or git commit id
OS version: x.x.x
Configuration: please attach config.h file where possible
Compiler and options (if you used a pre-built binary, please indicate how you obtained it):
Additional environment information:

Peer device TLS stack and version
OpenSSL|GnuTls|Chrome|NSS(Firefox)|SecureChannel (IIS/Internet Explorer/Edge)|Other
Version:

Expected behavior

Actual behavior

Steps to reproduce

Enhancement\Feature Request

Justification - why does the library need this feature?

Suggested enhancement

##
Question

Please first check for answers in the [mbed TLS knowledge Base](https://tls.mbed.org/kb), and preferebly file an issue in the [mbed TLS support forum](https://tls.mbed.org/discussions)
-----BEGIN CERTIFICATE-----
MIICHzCCAaWgAwIBAgIBCTAKBggqhkjOPQQDAjA+MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EwHhcN
MTMwOTI0MTU1MjA0WhcNMjMwOTIyMTU1MjA0WjA0MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxEjAQBgNVBAMTCWxvY2FsaG9zdDBZMBMGByqGSM49AgEG
CCqGSM49AwEHA0IABDfMVtl2CR5acj7HWS3/IG7ufPkGkXTQrRS192giWWKSTuUA
2CMR/+ov0jRdXRa9iojCa3cNVc2KKg76Aci07f+jgZ0wgZowCQYDVR0TBAIwADAd
BgNVHQ4EFgQUUGGlj9QH2deCAQzlZX+MY0anE74wbgYDVR0jBGcwZYAUnW0gJEkB
PyvLeLUZvH4kydv7NnyhQqRAMD4xCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQb2xh
clNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBFQyBDQYIJAMFD4n5iQ8zoMAoG
CCqGSM49BAMCA2gAMGUCMQCaLFzXptui5WQN8LlO3ddh1hMxx6tzgLvT03MTVK2S
C12r0Lz3ri/moSEpNZWqPjkCMCE2f53GXcYLqyfyJR078c/xNSUU5+Xxl7VZ414V
fGa5kHvHARBPc8YAIVIqDvHH1A==
-----END CERTIFICATE-----

```
-----BEGIN CERTIFICATE-----
MIIDhzCCAm+gAwIBAgIBADANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UECgwIUG9sYXJTU0wxGTAXBgNVBAMMEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTcwNTA0MTY1NzAxWhcNMjcwNTA1MTY1NzAxWjA7MQswCQYDVQQGEwJOTDERMA8G
A1UECgwIUG9sYXJTU0wxGTAXBgNVBAMMEFBvbGFyU1NMIFRlc3QgQ0EwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDA3zf8F7vglp0/ht6WMn1EpRagzSHx
mdTs6st8GFgIlKXsm8WL3xoemTiZhx57wI053zhdcHgH057Zk+i5clHFzqMwUqny
50BwFMtEonILwuVA+T7lpg6z+exKY8C4KQB0nFc7qKUEkHHxvYPZP9al4jwqj+8n
YMPGn8u67GB9t+aEMr5P+1gmIgNb1LTV+/Xjli5wwOQuvfwu7uJBVcA0Ln0kcmnL
R7EUQIN9Z/SG9jGr8XmksrUuEvmEF/Bibyc+E1ixVA0hmnM3oTDPb5Lc9un8rNsu
KNF+AksjoBXyOGVkCeoMbo4bF6BxyLObyavpw/LPh5aPgAIynplYb6LVAgMBAAGj
gZUwgZIwHQYDVR0OBBYEFLRa5KWz3tJS9rnVppUP6z68x/3/MGMGA1UdIwRcMFqA
FLRa5KWz3tJS9rnVppUP6z68x/3/oT+kPTA7MQswCQYDVQQGEwJOTDERMA8GA1UE
CgwIUG9sYXJTU0wxGTAXBgNVBAMMEFBvbGFyU1NMIFRlc3QgQ0GCAQAwDAYDVR0T
BAUwAwEB/zANBgkqhkiG9w0BAQUFAAOCAQEAfDd5khSv/+K3De9qmH/ID3CVapGS
EN5MlXS5vvGCjZSA41MuXkUl11akKHXQ9aLlp85OZUdGbfQ5wwCoj/MymbT4fES2
1dI8O1oI3PZI/0dqEvQETlIwSoZV2c/oaPRfh2E99v2+8FNIaZOfV2MX1n9+6AdO
W2nlK2oklozXSYg6KWtISr8N8Ofew2LQ9+riFlrrdaxsr8CoJqPqMDTq7FUmkDmO
oHize/h9bFksIunKoVQHa8P4w/W9bnR69nziyhZotbwOOkAWVnIyEM9QnaKWXeIy
rP6ewcTQjNYkguHJ8RY9rW+5bdaSY4EljSqZ3P3F+zo8P6sVi3qSlai5lQ==
-----END
 CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIICDTCCAXagAwIBAgIETZt8lzANBgkqhkiG9w0BAQUFADBCMUAwPgYDVQQDEzdP
cGVuVlBOIFdlYiBDQSAyMDExLjA0LjA1IDIwOjMzOjI3IFVUQyBhc2RlbW8ueW9u
YW4ubmV0MB4XDTExMDMyOTIwMzMyN1oXDTIxMDQwMjIwMzMyN1owQjFAMD4GA1UE
AxM3T3BlblZQTiBXZWIgQ0EgMjAxMS4wNC4wNSAyMDozMzoyNyBVVEMgYXNkZW1v
LnlvbmFuLm5ldDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA38U3wA/eTGN/
/AJHo2OsEHjLdO9k3Mo5QcShvg+6IoAThD7HEyOYm4Ild8s4+eEy2i9ecWvMKG6M
YSO+GwG9xOd9wDFtODpF+z6rIt8a4bLbQHcsp9Ccu+ZmjxkJkmxOCz774lxETArX
SaksAB5P6Web/LwKUv/Iy9crRM9HzSECAwEAAaMQMA4wDAYDVR0TBAUwAwEB/zAN
BgkqhkiG9w0BAQUFAAOBgQARCDFYCb9n151hgwitxzbuacIVDqIH8EouV2VBqlNR
tj8q1maliDE3pW7WRAwMi5i3+5c0auKwhTGESsBPjasd5QnjqXOkRbcZhkeVQ1ln
6NEn6xC+M+H2LGVHSSropcGa8olLlo98LrsFuHVHMewTs7SK2lc+7rU/ILec3ymj
og==
-----END CERTIFICATE-----
set(libs
  mbedtls
)

if(USE_PKCS11_HELPER_LIBRARY)
  set(libs ${libs} pkcs11-helper)
endif(USE_PKCS11_HELPER_LIBRARY)

if(ENABLE_ZLIB_SUPPORT)
  set(libs ${libs} ${ZLIB_LIBRARIES})
endif(ENABLE_ZLIB_SUPPORT)
```

```
add_executable(selftest selftest.c)
target_link_libraries(selftest ${libs})

add_executable(benchmark benchmark.c)
target_link_libraries(benchmark ${libs})

add_executable(ssl_cert_test ssl_cert_test.c)
target_link_libraries(ssl_cert_test ${libs})

add_executable(udp_proxy udp_proxy.c)
target_link_libraries(udp_proxy ${libs})

install(TARGETS selftest benchmark ssl_cert_test udp_proxy
    DESTINATION "bin"
    PERMISSIONS OWNER_READ OWNER_WRITE OWNER_EXECUTE GROUP_READ
GROUP_EXECUTE WORLD_READ WORLD_EXECUTE)
Test vector ARC4 [Cryptlib]
mbedtls_arc4_crypt:"0000000000000000":"0123456789abcdef":"7494c2e7104b0879"

Test vector ARC4 [COMMERCE]
mbedtls_arc4_crypt:"dcee4cf92c":"618a63d2fb":"f13829c9de"

Test vector ARC4 [SSH ARCFOUR]
mbedtls_arc4_crypt:"527569736c696e6e756e206c61756c75206b6f727669737373616e692c2074e4686be470e4696
4656e2070e4e46c6ce42074e47973696b75752e204b6573e479f66e206f6e206f6e6e69206f6d616e616e692c206b617
36b6973617675756e206c61616b736f7420766572686f75752e20456e206d6120696c6f697473652c20737572652068
756f6b61612c206d75747461206d657473e46e2074756d6d757573206d756c6c652074756f6b61612e205075756e746
f2070696c76656e2c206d692068756b6b75752c207369696e746f20766172616e207475756c6973656e2c206d69206e
756b6b75752e2054756f6b7375742076616e616d6f6e206a61207661726a6f74207665656e2c206e69697374e420737
964e46d656e69206c61756c756e207465656e2e202d2045696e6f204c65696e6f":"29041972fb42ba5fc7127712f1382
9c9":"358186999001e6b5daf05eceeb7eee21e0689c1f00eea81f7dd2caaee1d2763e68af0ead33d66c268bc946c484fbe
94c5f5e0b86a59279e4f824e7a640bd223210b0a61160b7bce986ea65688003596b630a6b90f8e0caf6912a98eb87217
6e83c202caa64166d2cce57ff1bca57b213f0ed1aa72fb8ea52b0be01cd1e412867720b326eb389d011bd70d8af035fb0
d8589dbce3c666f5ea8d4c7954c50c3f340b0467f81b425961c11843074df620f208404b394cf9d37ff54b5f1ad8f6ea7d
a3c561dfa7281f964463d2cc35a4d1b03490dec51b0711fbd6f55f79234d5b7c766622a66de92be996461d5e4dc878ef9
bca030521e8351e4baed2fd04f9467368c4ad6ac186d08245b263a2666d1f6c5420f1599dfd9f438921c2f5a463938ce0
982265eef70179bc553f339eb1a4c1af5f6a547f"

Test
 Vector ARC4 [RFC6229 40-bit]
mbedtls_arc4_crypt:"0000000000000000000000000000000000000000":"0102030405
":"b2396305f03dc027ccc3524a0a1118a86982944f18fc82d589c403a47a0d0919"

Test Vector ARC4 [RFC6229 56-bit]
mbedtls_arc4_crypt:"00000000000000000000000000000000000000000000000000000000":"0102030405
0607":"293f02d47f37c9b633f2af5285feb46be620f1390d19bd84e2e0fd752031afc1"

Test Vector ARC4 [RFC6229 64-bit]
```

mbedtls_arc4_crypt:"00000000000000000000000000000000000000000000000000000000000000000000":"0102030405060708":"97ab8a1bf0afb96132f2f67258da15a88263efdb45c4a18684ef87e6b19e5b09"

Test
Vector ARC4 [RFC6229 128-bit]
mbedtls_arc4_crypt:"0000000000000000000000000000000000000000000000000000000000000000":"0102030405060708090a0b0c0d0e0f10":"9ac7cc9a609d1ef7b2932899cde41b975248c4959014126a6e8a84f11d1a9e1c"

TMP
mbedtls_arc4_crypt:"1400002433c96cfa5c53a65184fcba83d9793f42522f94e49bf25edcb7a23c9eaae5ca84f6ee6da8":"5e58b1ad80":"e9a3d07ea1a3eac9fd73dcb14c409f2d434a72b6aa077e0924bcffc236f55d2d372b289707571531"

ARC4 Selftest
depends_on:MBEDTLS_SELF_TEST
arc4_selftest:
0I0*H=*H=2y}=IkO X"-{K)Q[$t
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTgwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTkwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQJyRCHND78
KxZHoHHdOTjPuD6HjHPnEKX8apblUpETDJuLW7YR3V8Q0dTac+JHiR6e2l4DlDbf
5bTiyFoAzw9yo4GJMIGGMB0GA1UdDgQWBBRQMc94kTqW+zQO3lo2WMI/81k3czBX
BgNVHSMEUDBOgBSDbIpYntlhJ0GgIsyd75XRhlC18qEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTE3ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgIzGOZqJRmvygzvLm8zxZFyoNpcT7e26H
nZd5xFIzEakCIHGYcUXzt+owSVlLmrlW8gQcB81ErQbxuBTAsvpaaKSS
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTcwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTgwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASsc/JkNcYf
bMgpOfrL5kKOGxOJaGS6SQIeNO33UeBpToe1bU2acN652xjvcGo0fJEtxg2fcPHR
hTnGMBD1u1N2o4GJMIGGMB0GA1UdDgQWBBSDbIpYntlhJ0GgIsyd75XRhlC18jBX
BgNVHSMEUDBOgBSnjWvpWxZcFnfQ2KGtCg/u6fT/D6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTE2ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAJo2NXfJU1sK6SVTu4OV21FKITlXntMi
oenYMsBjzO8oAiEAidSELcLjjAHi3mfBARvCgKlRhmbNEMCHQT7Ha7ZQoRw=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTYwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTcwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAARrISq2zO9m
D29YCLHB56FdU/RINtRhfeLtM+u5o3HaAnopy0S98RzuEGELjpzr8ZI6kkMMZsj8
nFZQF8HfuE0go4GJMIGGMB0GA1UdDgQWBBSnjWvpWxZcFnfQ2KGtCg/u6fT/DzBX

BgNVHSMEUDBOgBRTw3K0Psy3u/6+3KKSoaQqJnPvPqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTE1ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgDgXjoc6FfMF5W0NziV6vx2BOPNWav01Z
ynEP4h9ULnUCIQC1rU4sEId3UdjzTKhpSGTKtaOuPG+b0YdEMPimI4jmVw==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTUwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTYwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQ7Vsp7JmDN
kgPh/+zmIPkd7o0xot/WPMFn3uAsGtsU385MF0fmhfFLhRbbH9h4JjYHj8y0spU3
buUXhftvAZVbo4GJMIGGMB0GA1UdDgQWBBRTw3K0Psy3u/6+3KKSoaQqJnPvPjBX
BgNVHSMEUDBOgBR1mXlrdW5rx1VnqMMnUBXo0WWGWqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTE0ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAMJnGjE9v3SjuGfi0jNByrwyNfhlTHMh
FhPQidNrDpXwAiEAqYtNiV8t9RrAa9GC6FWDuJpvIiU6FsE+lFq6uIq/J2E=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTQwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTUwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQlKUiMoSss
/hsTasedqdB2BCOGJhTt0hgUGeUnWNZ1svO4yn0GkFHZ08++fl2MKqjpj+VXq0JS
FFyGUOgmgi3Ho4GJMIGGMB0GA1UdDgQWBBR1mXlrdW5rx1VnqMMnUBXo0WWGWjBX
BgNVHSMEUDBOgBRNsJB++ccSBmbCCKBxi4CjXROBk6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTEzggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAKYOIo+fdCQRqpH4LN8qUK1aKzKmWGxS
fGzEEkg/29bMAiAl95cmucoCDMq2Ab8Coc0dEqyJ6+rAPMLBCbGawyiW6A==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTMwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTQwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATRMZN0RHzP
donNmZuq9XPhzvQ52TaokxT39qpQtlFyvUuEGKrLoNvdcpARaA0rGput6RLAQOVU
iNVlJ3Ipj789o4GJMIGGMB0GA1UdDgQWBBRNsJB++ccSBmbCCKBxi4CjXROBkzBX
BgNVHSMEUDBOgBTmVnUSF2MYwws/nCMv7b1wJVkDmqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTEyggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgVfuLpjp08AaxKWf6cuZUUCRd7CojSS1I
71hzeUyFS+sCIQDNJI6P/pBbiHgTaGlBAgfcEfmxmbY0n4xZndtxIkmyVA==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTIwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx

DTALBgNVBAMMBENBMTMwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATrkzCJLznh
lhnsv1RXB9kfeaD+cIruPQ0cItBDGpdvD8xbBVvQci4+RG2RVUCSWRhkFYjSsUSM
0QHMQnBFlhw2o4GJMIGGMB0GA1UdDgQWBBTmVnUSF2MYwws/nCMv7b1wJVkDmjBX
BgNVHSMEUDBOgBTZTtbi+j0Sm/Zs/+gTkWdASpQzfqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTExggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgWsm+rHJgwUEyNm8EKbEds5yurpp5/3y5
PsvXJVDqxogCIQDUP0Jcl3A907CE2tPVXSgD6LQ6CPu19mixemPw60yijA==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTEwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTIwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATDE9LPlLPc
gZ3b0BchR/AkhNEP9HAavwYadJIyzoPo5edCVnboQH786jsZwZNZoC0gHDAhCmGc
IfRenISAoVuPo4GJMIGGMB0GA1UdDgQWBBTZTtbi+j0Sm/Zs/+gTkWdASpQzfjBX
BgNVHSMEUDBOgBSOSt6ePyMRT6PGMaIi7FqNX9MKtKEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTEwggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgYYF5AnRV7eh2hLD5Dz//pceMTKz9Ls46
E6DxvbfDHikCIFttlGrOCZVyS4ocsjuKIELVUX5qfygI0sn4kU3qCTs2
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTAwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATZwR+WK6NB
F/7riFdN63c8hjYddZRR4lrzVNPwiBQxnnxwpPyrD9A6aPPmLc6SqGOJW4ZGVCco
IBze9RJVeiB9o4GJMIGGMB0GA1UdDgQWBBSOSt6ePyMRT6PGMaIi7FqNX9MKtDBX
BgNVHSMEUDBOgBQtxZSLJAkEz+2RKMQexM6EtsfgcqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA5ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgN//NqM0FrkrMjmxoeCY9DgxkH2R6sQ4d
NgtwCZAIqEICIBs4vupaVcuvni9tltbP26wi7c0FR+blZuo5DPIA3SVe
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDkwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTAwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAR6jlGKbJd5
hiDxN789gkOcwpyHI9wRwCrADAOwOkMePBPRlwGdm7mw7Z/EAmu26zRm/hcyrs4M
qk2LabDjPI9Xo4GJMIGGMB0GA1UdDgQWBBQtxZSLJAkEz+2RKMQexM6EtsfgcjBX
BgNVHSMEUDBOgBT6gyXHzPIPYc1Vr1aGiLLeMh4HpqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA4ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgP7S8vFstfUBdNe6ym5GYG5Q+aBVEKqRs
fVW7HNUktSYCIQDo6Jua6o/DJbrpq4qYWq5gv4yGyzPTN+3IaKrEICdaaw==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G

A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDgwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDkwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAR7ZB16+t6E
sfahGyKUGJW5mezkzjdaYvc4lbJaKNRwFRfc3F/fmNOSsUFSg/F0N+vUE+doKiPC
8wRwLzvm4s+5o4GJMIGGMB0GA1UdDgQWBBT6gyXHzPIPYc1Vr1aGiLLeMh4HpjBX
BgNVHSMEUDBOgBS40mLt93U8Sh8ZGiDVAhRSiBPcXqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA3ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgO4el1ZPhlIli/qNR2SIEiuvs5Mmy868i
N2Rv5X/VxIECIA/8rUALQxW38XSdBVX3e/jzu7ju47n1YwEqD9K9WdVv
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDcwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDgwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAARpQeQ/YGQj
nl7Szo6WStJ1u7xunTL5jBkXH8aAVSm0qiX4AD/7YPxa5EnGzZdLTn25vQVnfQAG
pMx8P1lYiGYCo4GJMIGGMB0GA1UdDgQWBBS40mLt93U8Sh8ZGiDVAhRSiBPcXjBX
BgNVHSMEUDBOgBREq5J3toJPxZ3O+ssJ5vkkU0RJE6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA2ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhANwGf+F4a+kmXWz8UjSpRkaToTV6EFWw
/Tjzj0tQhDoAAiEA19RxeWOVBBpM6LOHg6v5Lf54YN1snkLf+sEXyZCuWQQ=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDYwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDcwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASNOj4d4MEA
7p/3miijqG4ToE4opKPAm+3BTIGrJTYT14++TSiUICl0ASXj+xeUcLMIaXTN042s
LsHxpShzQaL0o4GJMIGGMB0GA1UdDgQWBBREq5J3toJPxZ3O+ssJ5vkkU0RJEzBX
BgNVHSMEUDBOgBSjovYaC/m6Li9Tp0V9iZRs9267Q6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA1ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAKGcf+c442c/XiwubbaiQvsoZ7EoVxuM
oKmia0gPyBNkAiEA83asjJ5FDXQuLyZpczviXrbmqgCPOfYadtvkc0cxMis=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDUwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDYwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASA9qWoAUHr
nn+3kxyNrjPJk82WDLimW21RN51uxpobadv8YgGEDRdP+Ok+uRqQSUsA6ZXfF3iG
r2GjfQ3wMDH8o4GJMIGGMB0GA1UdDgQWBBSjovYaC/m6Li9Tp0V9iZRs9267QzBX
BgNVHSMEUDBOgBTXh06MAV9S4l4lG1TKOrKRBh4qn6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA0ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgcjZNFWJtlDmoPZbAxqsGczRYK0lfPgu6
g1H7pp0ce+wCIDj9BRZM2OB9EF0e+MDKGjyZGfvfrL6Ir47x/KrM6H8T

-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDQwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDUwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQEdT0OFf5G
UcrgX2XllCyJzP94NZ464GsgB6psNLsDeL+j7AU+oJy7VLvW/lHh3ODgl08Z9bhq
LFBmNjnHbm8Qo4GJMIGGMB0GA1UdDgQWBBTXh06MAV9S4l4lG1TKOrKRBh4qnzBX
BgNVHSMEUDBOgBQox4F1NsZunlsduoGvzIgRSYfB36EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAzggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAIW++zqDZlLLUk/emePohdNOp5JO3wS9
XvkBJ6Wua7GBAiAdx+EKmdjVrwnzrQltTgnmSfGMXhKNYifK3uD83W3pcQ==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDMwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDQwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQUXDgcUVNT
9hovbZE5HL6rjOb7C55wEuWKThV/CcZ4rWrXx7VXHYdD/R3aDA7JSvYpm2sTok4i
sblDzhZM/GDNo4GJMIGGMB0GA1UdDgQWBBQox4F1NsZunlsduoGvzIgRSYfB3zBX
BgNVHSMEUDBOgBQApzZdtBdD3dLxouQpr/aDiVttd6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAyggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgAkiNhqFAZXSUWEDK91OZvQGdeZOtd6mC
+Wv3fGk3t28CIEKOwidkUTUaiPdZ4efmAr+CEeGzdq27ob2S+nqqHqgV
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDIwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDMwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQRDXDNIi1p
ereudhqwa2LslXgsxnB63Hu5y5lg+1WPruIYPzD/Ho0APveVdzFLVji19+bE4+tF
PYL1SpsN1WfWo4GJMIGGMB0GA1UdDgQWBBQApzZdtBdD3dLxouQpr/aDiVttdzBX
BgNVHSMEUDBOgBT5RCgQ0AlZTQbfFB2+6+w0XRvydaEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAxggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAOnd+7bAofkHVa4KFNjv3TCegw1lrhuM
8Of8wgvrTEGoAiEAsS8iKMpSfXH4D0egg4gLamE6akde965rDtySU+ve9lg=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDEwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDIwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQWHpv1i6lf
wvNPOP5ka6S0n55EvzoaYK6pbTXP6yMOW/4XZSPKx5Zoq4FMe0cKzGIIFL1rzj1V
2czYB+qvLhyio4GJMIGGMB0GA1UdDgQWBBT5RCgQ0AlZTQbfFB2+6+w0XRvydTBX
BgNVHSMEUDBOgBSh3uHkX5nj86yFEFwjscSWM40P+qEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggEBMAwGA1UdEwQF

MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAI7unGW/gr9tOc3i+dF5N815srgh+FrX
oj9Et74EcSpTAiBubv+vOH0DE0gmYI11HeAIgutWqqMIC72dZlwTF/Vi3g==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB3jCCAYWgAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDAwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQznn9zHHwL
GO8VR4W9V7vMlxCdoojzEOiX5Y6JtPtFOz866ueHY6zoN0/mJ6DnqnSXilJIUUeW
6eGfqmka7nxko4GRMIGOMB0GA1UdDgQWBBSh3uHkX5nj86yFEFwjscSWM40P+jBf
BgNVHSMEWDBWgBQlFYvU5WboI4fcdPoiQs8/fPHZraEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggkA/KCWhcqToHAw
DAYDVR0TBAUwAwEB/zAKBggqhkjOPQQDAgNHADBEAiBasbuinP+pJTU4oDCVD8zQ
1rJBDSOKIEyWu84/D6Hj6wIgVMPUoO01bPhzllAa/gW8Xk/daey09SBgN3AT9pWU
TDA=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIBpTCCAUugAwIBAgIJAPygloXKk6BwMAoGCCqGSM49BAMCMC8xCzAJBgNVBAYT
AlVLMREwDwYDVQQKDAhtYmVkIFRMUzENMAsGA1UEAwwEQ0EwMDAeFw0xNzA2MjIx
MTUwMzJaFw0yNzA2MjMxMTUwMzJaMC8xCzAJBgNVBAYTAlVLMREwDwYDVQQKDAht
YmVkIFRMUzENMAsGA1UEAwwEQ0EwMDBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IA
BFW41/qAwAPpy+Txdc7PKmzZsq9CPiujKU4vpF1ekXnGx2HP420QobwBVVWhkzRm
LwdboH2j65dcCKjQ7mv/dxKjUDBOMB0GA1UdDgQWBBQlFYvU5WboI4fcdPoiQs8/
fPHZrTAfBgNVHSMEGDAWgBQlFYvU5WboI4fcdPoiQs8/fPHZrTAMBgNVHRMEBTAD
AQH/MAoGCCqGSM49BAMCA0gAMEUCIQC7iRcVzwMyfVK5imirJ7MqJQ04euH4CLOt
IZ+SNfaERAIgSU0MWFDosVEIpg8YMqIHeF7Mg4ZyH6+fGazJgVLttUY=
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-CBC,F87FE1C0FB9B3E77

1NbOyRx5kBWeXy93eCXyidDpR3pbfgGWIIgXVCVE4/ZXgEt14A23YndZeI5OSxvG
JWhqZ+VuiRsxeKAjo+xf4bnKLArvbshhzUKCEVsCP1d2d1xfgjsnyr8tqNiJE0F6
7Nimjcrpw/udCk2RBVyshN9kiPBbnA+XUdOHfEnbdkqDsS5DGjq7H1kBZuHhTQa8
Xv6ta3kbI1BGiqKDhH2H9iJlZMwpVQuJs+HqcqNEhsPm0V4kp0S3PZMbYVKpEtDO
vh9CHprQy/nlHfq7ZAs9/2HN4/OT/5kw4JM9qQy7eo/6FX2yh39Lyz8u7PXLaVgM
pwOiFb+zvegYts5aCXyM1nBUu9NFPDQNDytjXOhbWL0hEr1RzgK67f5QYIxWgGCK
St4moIn7J5BifViNdp7j/RXCoCmda3Zv5PiRw83yScSlzgDdTNpm/70jp8pGSxEn
Ib768zYEcYeeKyPar210Nh9abySPpkFFaujN4do5wujboC0VPz73M6eTeZ6iOUgR
cX9WwkfRj6G6VQfM6xAZdOkQ2cj6M4YRze1RKLhqo0+gre76FLn8Kzf/Hjrp/0iy
0flr/6BwLxGV49vMUCesJ9oqE/frru9Y89cOwbgcHxKJ24Oz+64OUPyeSxDMElZ8
lXiNk3aBEuLdBOKJ8B9kyKuxNqwDoqhCsrc77Gjio+q24w+G2+KAzBEup4S9cYgp
FiSvK8sizKINfE14f9HA60MJJzyEjTUuL7+ioL7xHGtIkdWbs/Qp7KxliH6qoIUv
VUsT6VS1nWLDyTyMbcjMx1odRsWrLwLqIsvNIcGGwe+P4sm4LivNnQ==
-----END RSA PRIVATE KEY-----

Timing selftest
timing_selftest:
-----BEGIN PUBLIC KEY-----
MIGbMBQGByqGSM49AgEGCSskAwMCCAEBDQOBggAEOLfskrYcXGx/vCik7HWdSPzU
4uN03v1cSWilTb73UQ5ReIb7/DjqOapSk1nXCnFWw108usfOd2vbJR3WS85xI0Qk
7nBJ7tBy8NvE15mW4XXVV+JjdjrpcJXAgec+fbLjitw9TJoEh7Ht6HbcH8phyQLp
odhyK4YSko8YokhFWRo=
-----END PUBLIC KEY-----
00 0
*H=0>10 UNL10U
PolarSSL10UPolarssl Test EC CA0
130924155204Z
230922155204Z0410 UNL10U
PolarSSL10U localhost0Y0*H=*H=B7Vv Zr>Y- n|th"YbN#/4]]kw
U*00 U00UPaecF0nU#g0em $I?+x~$6|B@0>10 UNL10U
PolarSSL10UPolarssl Test EC CA C~bC0
*H=h0e1,\d
Na1ssT]/!)5>90!6]'%;5%Y^|f{Os!R*03vz)
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
   <Configuration>Release</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\pkey\pk_decrypt.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">

   <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
 </ItemGroup>

```
 <PropertyGroup Label="Globals">
  <ProjectGuid>{1EC6CBA3-6187-D456-D9B7-A35399395D71}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>pk_decrypt</RootNamespace>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
/>
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
```

```
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
     <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
```

```
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
```

```
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
 <Import
 Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
    <Configuration>Debug</Configuration>
    <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
    <Configuration>Debug</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
    <Configuration>Release</Configuration>
    <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
    <Configuration>Release</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\ssl\dtls_server.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">

    <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid>{BFE89EAA-D98B-34E1-C5A4-4080F6FFE317}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>dtls_server</RootNamespace>
 </PropertyGroup>
```

```
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
   <UseDebugLibraries>true</UseDebugLibraries>
   <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
   <UseDebugLibraries>true</UseDebugLibraries>
   <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
    <ConfigurationType>Application</ConfigurationType>
   <UseDebugLibraries>false</UseDebugLibraries>
   <WholeProgramOptimization>true</WholeProgramOptimization>
   <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
   <UseDebugLibraries>false</UseDebugLibraries>
   <WholeProgramOptimization>true</WholeProgramOptimization>
   <CharacterSet>Unicode</CharacterSet>
   <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
 />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
    <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
```

```
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
     <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
```

<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
<AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
</Link>
<ProjectReference>
<LinkLibraryDependencies>false</LinkLibraryDependencies>
</ProjectReference>
</ItemDefinitionGroup>
<ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
<ClCompile>
<WarningLevel>Level3</WarningLevel>
<PrecompiledHeader>
</PrecompiledHeader>
<Optimization>MaxSpeed</Optimization>
<FunctionLevelLinking>true</FunctionLevelLinking>
<IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
<AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
</ClCompile>
<Link>
<SubSystem>Console</SubSystem>
<GenerateDebugInformation>true</GenerateDebugInformation>
<EnableCOMDATFolding>true</EnableCOMDATFolding>
<OptimizeReferences>true</OptimizeReferences>
<AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
</Link>
</ItemDefinitionGroup>
<ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
<ClCompile>
<WarningLevel>Level3</WarningLevel>
<PrecompiledHeader>
</PrecompiledHeader>
<Optimization>MaxSpeed</Optimization>
<FunctionLevelLinking>true</FunctionLevelLinking>
<IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
<AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
</ClCompile>
<Link>
<SubSystem>Console</SubSystem>
<GenerateDebugInformation>true</GenerateDebugInformation>
<EnableCOMDATFolding>true</EnableCOMDATFolding>
<OptimizeReferences>true</OptimizeReferences>
<AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>

```
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
   </Link>
 </ItemDefinitionGroup>
 <Import
 Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTEwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTIwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATDE9LPlLPc
gZ3b0BchR/AkhNEP9HAavwYadJIyzoPo5edCVnboQH786jsZwZNZoC0gHDAhCmGc
IfRenISAoVuPo4GJMIGGMB0GA1UdDgQWBBTZTtbi+j0Sm/Zs/+gTkWdASpQzfjBX
BgNVHSMEUDBOgBSOSt6ePyMRT6PGMaIi7FqNX9MKtKEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTEwggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgYYF5AnRV7eh2hLD5Dz//pceMTKz9Ls46
E6DxvbfDHikCIFttlGrOCZVyS4ocsjuKIELVUX5qfygI0sn4kU3qCTs2
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIBqTCCAUygAwIBAgIBWzAMBggqhkjOPQQDAgUAMDExDzANBgNVBAMTBlJvb3Qg
OTERMA8GA1UEChMIbWJlZCBUTFMxCzAJBgNVBAYTAlVLMB4XDTAxMDEwMTAwMDAw
MFoXDTMwMTIzMTIzNTk1OVowMTEPMA0GA1UEAxMGUm9vdCA5MREwDwYDVQQKEwht
YmVkIFRMUzELMAkGA1UEBhMCVUswWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATh
D2SmdS6D7cYi2vGMyuCdol/OOUN2di2pS2wfSI/MsY/Z4O9iNHqbXQP6l+hcT5ap
daycs7r6ZPNqmWM7b16go1MwUTAPBgNVHRMECDAGAQH/AgEAMB0GA1UdDgQWBBRb
zVrcAxddj0i0DEqvTGT8F37bizAfBgNVHSMEGDAWgBRbzVrcAxddj0i0DEqvTGT8
F37bizAMBggqhkjOPQQDAgUAA0kAMEYCIQDbrSV4ndH0vAR3HqJfBn8NT8zdvMjB
qSJes6Qwa42b2wIhAKyoH0H+b1Svw8pMkvUYF4ElH5Cnn7gxb7Wl3arc0+hQ
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDUjCCAjqgAwIBAgIBATANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTEwMjEyMTQ0NDA2WhcNMjEwMjEyMTQ0NDA2WjA8MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxGjAYBgNVBAMTEVBvbGFyU1NMIFNlcnZlciAxMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqQIfPUBq1VVTi/027oJlLhVhXom/
uOhFkNvuiBZS0/FDUEeWEllkh2v9K+BG+XO+3c+S4ZFb7Wagb4kpeUWA0INq1UFD
d185fAkER4KwVzlw7aPsFRkeqDMIR8EFQqn9TMO0390GH00QUUBncxMPQPhtgSVf
CrFTxjB+FTms+Vruf5KepgVb5xOXhbUjktnUJAbVCSWJdQfdphqPPwkZvq1lLGTr
lZvc/kFeF6babFtpzAK6FCwWJJxK3M3Q91Jnc/EtoCP9fvQxyi1wyokLBNsupk9w
bp7OvViJ4lNZnm5akmXiiD8MlBmj3eXonZUT7Snbq3AS3FrKaxerUoJUsQIDAQAB
o2AwXjAJBgNVHRMEAjAAMB0GA1UdDgQWBBQfdNY/KcF0dEU7BRIsPai9Q1kCpjAf
BgNVHSMEGDAWgBS0WuSls97SUva51aaVD+s+vMf9/zARBglghkgBhvhCAQEEBAMC
AEAwDQYJKoZIhvcNAQEFBQADggEBAJ28VuktjDGkUWcVpM/W+YjohFDay676Yozx
BbBLU3QZiDkcdXZbX/jOaKKBGWrjWiB6txchV4XrlvEtVtPgPrQLil2xaD20LOqJ
e/ZEFIAIndf06CAcimdQaPD6mww04v3gZw3cwPQd/aMQCw9tm93tyf6YU4uIh/o8
evG1ZBrNHRyiW18kbuueLNZ2daYQIISRJSIFrAERacfOvA8r7yXJCqZnB6AU5j9u
```

V+ySNW3sdZIOTfs1nWKU6SECWo72dd89Yvs7wCf3NSZNM2UemLeOjQOmZIHBiR8L
PAhDxhra5B/QBKaWeTVQohEvKz75pLAWouUGIKlgHiqJ4cvBGcg=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDWzCCAhKgAwIBAgIBFzA+BgkqhkiG9w0BAQowMaANMAsGCWCGSAFlAwQCBKEa
MBgGCSqGSIb3DQEBCDALBglghkgBZQMEAgSiBAICAOIwOzELMAkGA1UEBhMCTkwx
ETAPBgNVBAoTCFBvbGFyU1NMMRkwFwYDVQQDExBQb2xhclNTTCBUZXN0IENBMB4X
DTE0MDEyMDEzNTczNloXDTI0MDExODEzNTczNlowNDELMAkGA1UEBhMCTkwxETAP
BgNVBAoTCFBvbGFyU1NMMRIwEAYDVQQDEwlsb2NhbGhvc3QwgZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBAN0Rip+ZurBoyirqO2ptWZftTslU5A3uzqB9oB6q6A7C
uxNA24oSjokTJKXF9frY9ZDXyMrLxf6THa/aEiNzUnlGGrqgVyt2FjGzqK/nOJsI
i2OZOgol7kXSGFi6uZMa7dRYmmMbN/z3FAifhWVJ81kybdHg6G3eUu1mtKkL2kCV
AgMBAAGjgZIwgY8wCQYDVR0TBAIwADAdBgNVHQ4EFgQU7vPH9R8VpU1HicHTImOy
36fOvVEwYwYDVR0jBFwwWoAUtFrkpbPe0lL2udWmlQ/rPrzH/f+hP6Q9MDsxCzAJ
BgNVBAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEZMBcGA1UEAxMQUG9sYXJTU0wg
VGVzdCBDQYIBADA+BgkqhkiG9w0BAQowMaANMAsGCWCGSAFlAwQCBKEaMBgGCSqG
SIb3DQEBCDALBglghkgBZQMEAgSiBAICAOIDggEBADJExjfWWvL28lgj+GGgviqo
PHZLxI0pLQUnFJQ9Kpu6jxfICseBF00Z6BJE/RcYDpIie5GDt/8u/i6xB6Li29Pm
g5nANgd/Y3fFnW7d0ydVjiSnetlPuf/jTlWQl6mQTH2xqYu8J8d3JRxQdRiDYbVm
uywW2d6rksiqm6dPD5l4A5DcemcYo8f/1Ifj5WNDCV8/OHex+AnW2ccDvWAnVgSR
B2VpOXJzVFuBsuf4tGVm/2TUMSB6NcvFc6TeJk1kzbZxii4QjKXtH1SfrVP59iEe
l17NYAEWARjBpQWBiutRG+QM2et0sNiUBuWxTkvd0eSgencNysVAOsZqrqaX3CY=
-----END
CERTIFICATE-----
AES 128 GCM Encrypt and decrypt 0 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_128_GCM:"AES-128-GCM":128:0:-1

AES 128 GCM Encrypt and decrypt 1 byte
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_128_GCM:"AES-128-GCM":128:1:-1

AES 128 GCM Encrypt and decrypt 2 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_128_GCM:"AES-128-GCM":128:2:-1

AES 128 GCM Encrypt and decrypt 7 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_128_GCM:"AES-128-GCM":128:7:-1

AES 128 GCM Encrypt and decrypt 8 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_128_GCM:"AES-128-GCM":128:8:-1

AES 128 GCM Encrypt and decrypt 9 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_128_GCM:"AES-128-GCM":128:9:-1

AES 128 GCM Encrypt and decrypt 15 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_128_GCM:"AES-128-GCM":128:15:-1

AES 128
GCM Encrypt and decrypt 16 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_128_GCM:"AES-128-GCM":128:16:-1

AES 128 GCM Encrypt and decrypt 17 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_128_GCM:"AES-128-GCM":128:17:-1

AES 128 GCM Encrypt and decrypt 31 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_128_GCM:"AES-128-GCM":128:31:-1

AES 128 GCM Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_128_GCM:"AES-128-GCM":128:32:-1

AES 128 GCM Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_128_GCM:"AES-128-GCM":128:33:-1

AES 128 GCM Encrypt and decrypt 47 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_128_GCM:"AES-128-GCM":128:47:-1

AES 128 GCM Encrypt and decrypt 48 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_128_GCM:"AES-128-GCM":128:48:-1

AES
128 GCM Encrypt and decrypt 49 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_128_GCM:"AES-128-GCM":128:49:-1

AES 128 GCM Encrypt and decrypt 0 bytes in multiple parts
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_GCM:128:0:0

AES 128 GCM Encrypt and decrypt 1 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_GCM:128:1:0

AES 128 GCM Encrypt and decrypt 1 bytes in multiple parts 2

depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_GCM:128:0:1

AES 128 GCM Encrypt and decrypt 16 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_GCM:128:16:0

AES 128 GCM Encrypt and decrypt 16 bytes in multiple parts 2
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_GCM:128:0:16

AES 128 GCM Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_GCM:128:16:6

AES
128 GCM Encrypt and decrypt 22 bytes in multiple parts 2
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_GCM:128:0:22

AES 128 GCM Encrypt and decrypt 32 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_GCM:128:16:16

AES 128 GCM Decrypt test vector #1
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_AES_128_GCM:-
1:"d785dafea3e966731ef6fc6202262584":"d91a46205ee94058b3b8403997592dd2":"":"":"":"3b92a17c1b9c3578a6
8cffea5a5b6245":0:0

AES 128 GCM Decrypt test vector #2
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_AES_128_GCM:-
1:"9ab5c8ca905b5fe50461f4a68941144b":"96dd3927a96e16123f2e9d6b367d303f":"":"":"":"6e0c53ef":0:0

AES 128 GCM Decrypt test vector #3
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_AES_128_GCM:-
1:"b5fc7af605721a9cfe61c1ee6a4b3e22":"6b757d4055823d1035d01077666037d6":"":"":"":"e8c09ddd":0:MBEDT
LS_ERR_CIPHER_AUTH_FAILED

AES
128 GCM Decrypt test vector #4
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_AES_128_GCM:-
1:"03c0b4a6e508a8490db0d086a82c9db7":"ac52f6c1a05030321fa39f87e89fdb5e":"":"":"33316ca79d10a79f4fd038
593e8eef09625089dc4e0ffe4bc1f2871554fa6666ab3e7fe7885edef694b410456f3ec0e513bb25f1b48d95e4820c5972
c1aabb25c84c08566002dadc36df334c1ce86847964a122016d389ac873bca8c335a7a99bcef91e1b985ae5d488a2d7f7

8b4bf14e0c2dc715e814f4e24276057cf668172":"756292d8b4653887edef51679b161812":0:MBEDTLS_ERR_CIPHER_AUTH_FAILED

AES 128 GCM Decrypt test vector #5
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_AES_128_GCM:-
1:"2bc73fba942ff105823b5dccf6befb1c":"902c3e3b69b1ef8395d7281ff74cce38":"":"":"4adec0b4ac00325a860044d9f9519daa4f7c163229a75819b0fd7d8e23319f030e61dfa8eadabff42ea27bc36bdb6cad249e801ca631b656836448b7172c11126bad2781e6a1aa4f62c4eda53409408b008c057e0b81215cc13ddabbb8f1915f4bbab854f8b00763a530ad5055d265778cd3080d0bd35b76a329bdd5b5a2d268":"ebdd7c8e87fe733138a433543542d1":0:0

AES
128 GCM Decrypt test vector #6
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_AES_128_GCM:-
1:"0dd358bc3f992f26e81e3a2f3aa2d517":"d8c750bb443ee1a169dfe97cfe4d855b":"87cc4fd75788c9d5cc83bae5d764dd249d178ab23224049795d4288b5ed9ea3f317068a39a7574b300c8544226e87b08e008fbe241d094545c211d56ac44437d41491a438272738968c8d371aa7787b5f606c8549a9d868d8a71380e9657d3c0337979feb01de5991fc1470dfc59eb02511efbbff3fcb479a862ba3844a25aaa":"77949b29f085bb3abb71a5386003811233056d3296eb093370f7777dadd306d93d59dcb9754d3857cf2758091ba661f845ef0582f6ae0e134328106f0d5d16b541cd74fdc756dc7b53f4f8a194daeea9369ebb1630c01ccb307b848e9527da20a39898d748fd59206f0b79d0ed946a8958033a45bd9ae673518b32606748eb65":"":"a81d13973baa22a751833d7d3f94b3b1":0:0

AES 128 GCM Decrypt test vector #7
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_AES_128_GCM:-
1:"9a433c612d7e1bdff881e4d63ba8b141":"8b670cf31f470f79a6c0b79e73863ca1":"ce10758332f423228b5e4ae31efda7677586934a1d8f05d9b7a0dc4e2010ec3eaacb71a527a5fff8e787d75ebd24ad163394c891b33477ed9e2a2d853c364cb1c5d0bc317fcaf4010817dbe5f1fd1037c701b291b3a66b164bc818bf5c00a4c210a1671faa574d74c7f3543f6c09aaf117e12e2eb3dae55edb1cc5b4086b617d":"":"":"8526fd25daf890e79946a205b698f287":0:MBEDTLS_ERR_CIPHER_AUTH_FAILED

AES
128 GCM Decrypt test vector #8
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_AES_128_GCM:-
1:"69eedf3777e594c30e94e9c5e2bce467":"a3330638a809ba358d6c098e4342b81e":"5114e9983c96fecec3f7304ca42f52aa16cb7c6aadfb62ad537c93a3188835ca0703dad34c73cf96435b668b68a7a1d056931959316e8d3ab956bf64c4e07479c7767f9d488b0c0c351333ccf400b7e0be19a0fd173e3f2a1ae313f27e516952260fd2da9ab9daca478ebb93cd07d0b7503b32364d8e308d904d966c58f226bb":"208e6321238bf5c6e2ef55a4b8f531cbbfb0d77374fe32df6dd663486cf79beeed39bb6910c3c78dd0cc30707a0a12b226b2d06024db25dcd8a4e620f009cafa5242121e864c7f3f4360aaf1e9d4e548d99615156f156008418c1c41ff2bbc007cecf8f209c73203e6df89b32871de637b3d6af2e277d146ae03f3404d387b77":"df4e3f2b47cf0e8590228fcf9913fb8a5eb9751bba318fd2d57be68c7e788e04fabf303699b99f26313d1c4956105cd2817aad21b91c28f3b9251e9c0b354490fa5abfcea0065aa3cc9b96772eb8af06a1a9054bf12d3ae698dfb01a13f989f8b8a4bb61686cf3adf58f05873a24d403a62a092290c2481e4159588fea6b9a09":"5de3068e1e20eed469265000077b1db9":0:0

AES

128 GCM Decrypt test vector #9
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_AES_128_GCM:-
1:"45cc35311eedf0ba093bf901931a7036":"fed5084de3c348f5a0adf4c2fd4e848a":"5dc8d7525eaad035c19714ae1b1
e538cb66a4089027245351e0ad9297410fb3a0c1155407c10a8bb95a9ca624a9c9925dac003ee78926c6e90ff4ccdba10
e8a78bda1c4478162a0e302de5ff05fb0f94c89c3c7429fb94828bdcd97d21333c2ee72963ee6f056ce272b8bab007e65
3a42b01d1d2041ba627f169c8c0d32e6dae":"":"6e210914e4aed188d576f5ad7fc7e4cf7dd8d82f34ea3bcbdb7267cfd9
045f806978dbff3460c4e8ff8c4edb6ad2edba405a8d915729d89aab2116b36a70b54f5920a97f5a571977e0329eda6c6
96749be940eabfc6d8b0bbd6fbdb87657b3a7695da9f5d3a7384257f20e0becd8512d3705cc246ee6ca1e610921cf9260
3d79":"266a895fc21da5176b44b446d7d1921d":0:MBEDTLS_ERR_CIPHER_AUTH_FAILED

AES
192 GCM Encrypt and decrypt 0 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_192_GCM:"AES-192-GCM":192:0:-1

AES 192 GCM Encrypt and decrypt 1 byte
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_192_GCM:"AES-192-GCM":192:1:-1

AES 192 GCM Encrypt and decrypt 2 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_192_GCM:"AES-192-GCM":192:2:-1

AES 192 GCM Encrypt and decrypt 7 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_192_GCM:"AES-192-GCM":192:7:-1

AES 192 GCM Encrypt and decrypt 8 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_192_GCM:"AES-192-GCM":192:8:-1

AES 192 GCM Encrypt and decrypt 9 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_192_GCM:"AES-192-GCM":192:9:-1

AES
192 GCM Encrypt and decrypt 15 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_192_GCM:"AES-192-GCM":192:15:-1

AES 192 GCM Encrypt and decrypt 16 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_192_GCM:"AES-192-GCM":192:16:-1

AES 192 GCM Encrypt and decrypt 17 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_192_GCM:"AES-192-GCM":192:17:-1

AES 192 GCM Encrypt and decrypt 31 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_192_GCM:"AES-192-GCM":192:31:-1

AES 192 GCM Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_192_GCM:"AES-192-GCM":192:32:-1

AES 192 GCM Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_192_GCM:"AES-192-GCM":192:33:-1

AES 192 GCM Encrypt and decrypt 47 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_192_GCM:"AES-192-GCM":192:47:-1

AES
192 GCM Encrypt and decrypt 48 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_192_GCM:"AES-192-GCM":192:48:-1

AES 192 GCM Encrypt and decrypt 49 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_192_GCM:"AES-192-GCM":192:49:-1

AES 192 GCM Encrypt and decrypt 0 bytes in multiple parts
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_192_GCM:192:0:0

AES 192 GCM Encrypt and decrypt 1 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_192_GCM:192:1:0

AES 192 GCM Encrypt and decrypt 1 bytes in multiple parts 2
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_192_GCM:192:0:1

AES 192 GCM Encrypt and decrypt 16 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_192_GCM:192:16:0

AES 192 GCM Encrypt and decrypt
16 bytes in multiple parts 2
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_192_GCM:192:0:16

AES 192 GCM Encrypt and decrypt 22 bytes in multiple parts 1

depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_192_GCM:192:16:6

AES 192 GCM Encrypt and decrypt 22 bytes in multiple parts 2
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_192_GCM:192:0:22

AES 192 GCM Encrypt and decrypt 32 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_192_GCM:192:16:16

AES 192 GCM Decrypt test vector #1
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_AES_192_GCM:-
1:"806766a4d2b6507cc4113bc0e46eebe120eacd948c24dc7f":"4f801c772395c4519ec830980c8ca5a4":"":"":"":"8fa
16452b132bebc6aa521e92cb3b0ea":0:MBEDTLS_ERR_CIPHER_AUTH_FAILED

AES 192 GCM Decrypt test vector #2
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_AES_192_GCM:-
1:"be2f0f4ae4ab851b258ec5602628df261b6a69e309ff9043":"646a91d83ae72b9b9e9fce64135cbf73":"":"":"":"169e
717e2bae42e3eb61d0a1a29b":0:MBEDTLS_ERR_CIPHER_AUTH_FAILED

AES
192 GCM Decrypt test vector #3
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_AES_192_GCM:-
1:"1eb53aa548b41bfdc85c657ebdebdae0c7e525a6432bc012":"37ffc64d4b2d9c82dd17d1ad3076d82b":"":"":"":"34b
8e037084b3f2d":0:MBEDTLS_ERR_CIPHER_AUTH_FAILED

AES 192 GCM Decrypt test vector #4
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_AES_192_GCM:-
1:"c6a98102af3d875bcdebe594661d3a6b376970c02b11d019":"bea8cd85a28a2c05bf7406b8eef1efcc":"":"":"f2f80e
2c042092cc7240b598ab30fad055bce85408aa0f8cefaf8a7204f0e2acb87c78f46a5867b1f1c19461cbf5ed5d2ca21c96a
63fb1f42f10f394952e63520795c56df77d6a04cb5ad006ee865a47dc2349a814a630b3d4c4e0fd149f51e8fa846656ea5
69fd29a1ebafc061446eb80ec182f833f1f6d9083545abf52fa4c":"04b80f25ae9d07f5fd8220263ac3f2f7":0:0

AES 192 GCM Decrypt test vector #5
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_AES_192_GCM:-
1:"a249135c9f2f5a8b1af66442a4d4e101771a918ef8acee05":"80b6e48fe4a3b08d40c1636b25dfd2c4":"c62b39b937
edbdc9b644321d5d284e62eaa4154010c7a3208c1ef4706fba90223da04b2f686a28b975eff17386598ba77e212855692
f384782c1f3c00be011e466e145f6f8b65c458e41409e01a019b290773992e19334ffaca544e28fc9044a5e86bcd2fa5ad
2e76f2be3f014d8c387456a8fcfded3ae4d1194d0e3e53a2031":"b865f8dd64a6f51a500bcfc8cadbc9e9f5d54d2d27d81
5ecfe3d5731e1b230c587b46958c6187e41b52ff187a14d26aa41c5f9909a3b77859429232e5bd6c6dc22cf5590402476
d033a32682e8ab8dc7ed0b089c5ab20ab9a8c5d6a3be9ea7aa56c9d3ab08de4a4a019abb447db448062f16a533d41695
1a8ff6f13ed5608f77":"":"951c1c89b6d95661630d739dd9120a73":0:0

AES
192 GCM Decrypt test vector #6
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_AES_192_GCM:-
1:"23c201968def551817f20e49b09dbb5aae0033305bef68a0":"bd2952d215aed5e915d863e7f7696b3e":"77bc8af42d
1b64ee39012df5fc33c554af32bfef6d9182804dcfe370dfc4b9d059bdbc55f6ba4eacb8e3a491d96a65360d790864ba60
acf1a605f6b28a6591513ea3cfd768ff47aee242a8e9bdfac399b452231bfd59d81c9b91f8dc589ad751d8f9fdad01dd00
631f0cb51cb0248332f24194b577e5571ceb5c037a6d0bcfe8":"17d93c921009c6b0b3ecf243d08b701422983f2dcaec
9c8d7604a2d5565ed96ce5cddcb183cd5882f8d61d3202c9015d207fed16a4c1195ba712428c727601135315fc504e80
c253c3a2e4a5593fc6c4a206edce1fd7104e8a888385bbb396d3cdf1eb2b2aa4d0c9e45451e99550d9cfa05aafe6e7b531
9c73c33fd6f98db3c5":"23f35fac583897519b94998084ad6d77666e13595109e874625bc6ccc6d0c7816a62d64b02e6
70fa664e3bb52c276b1bafbeb44e5f9cc3ae028daf1d787344482f31fce5d2800020732b381a8b11c6837f428204b7ed2f
4c4810067f2d4da99987b66e6525fc6b9217a8f6933f1681b7cfa857e102f616a7c84adc2f676e3a8f":"bb9ba3a9ac7d63
e67bd78d71dc3133b3":0:0

AES
256 GCM Encrypt and decrypt 0 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_256_GCM:"AES-256-GCM":256:0:-1

AES 256 GCM Encrypt and decrypt 1 byte
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_256_GCM:"AES-256-GCM":256:1:-1

AES
256 GCM Encrypt and decrypt 2 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_256_GCM:"AES-256-GCM":256:2:-1

AES 256 GCM Encrypt and decrypt 7 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_256_GCM:"AES-256-GCM":256:7:-1

AES 256 GCM Encrypt and decrypt 8 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_256_GCM:"AES-256-GCM":256:8:-1

AES 256 GCM Encrypt and decrypt 9 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_256_GCM:"AES-256-GCM":256:9:-1

AES 256 GCM Encrypt and decrypt 15 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_256_GCM:"AES-256-GCM":256:15:-1

AES 256 GCM Encrypt and decrypt 16 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C

enc_dec_buf:MBEDTLS_CIPHER_AES_256_GCM:"AES-256-GCM":256:16:-1

AES 256 GCM Encrypt and decrypt 17 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_256_GCM:"AES-256-GCM":256:17:-1

AES
256 GCM Encrypt and decrypt 31 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_256_GCM:"AES-256-GCM":256:31:-1

AES 256 GCM Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_256_GCM:"AES-256-GCM":256:32:-1

AES 256 GCM Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_256_GCM:"AES-256-GCM":256:33:-1

AES 256 GCM Encrypt and decrypt 47 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_256_GCM:"AES-256-GCM":256:47:-1

AES 256 GCM Encrypt and decrypt 48 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_256_GCM:"AES-256-GCM":256:48:-1

AES 256 GCM Encrypt and decrypt 49 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_AES_256_GCM:"AES-256-GCM":256:49:-1

AES 256 GCM Encrypt and decrypt 0 bytes in multiple parts
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_256_GCM:256:0:0

AES
256 GCM Encrypt and decrypt 1 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_256_GCM:256:1:0

AES 256 GCM Encrypt and decrypt 1 bytes in multiple parts 2
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_256_GCM:256:0:1

AES 256 GCM Encrypt and decrypt 16 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_256_GCM:256:16:0

AES 256 GCM Encrypt and decrypt 16 bytes in multiple parts 2
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_256_GCM:256:0:16

AES 256 GCM Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_256_GCM:256:16:6

AES 256 GCM Encrypt and decrypt 22 bytes in multiple parts 2
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_256_GCM:256:0:22

AES
256 GCM Encrypt and decrypt 32 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_256_GCM:256:16:16

AES 128 GCM Decrypt test vector #0
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_AES_256_GCM:-
1:"2c186654406b2b92c9639a7189d4ab5ab0b9bb87c43005027f3fa832fd3507b1":"3a0324d63a70400490c92e7604a
3ba97":"":"":"":"4c61cd2e28a13d78a4e87ea7374dd01a":0:MBEDTLS_ERR_CIPHER_AUTH_FAILED

AES 128 GCM Decrypt test vector #1
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_AES_256_GCM:-
1:"c8ae011795c9a60ad7660a31fe354fa6f7e9c2724d7a126436291680cd95c007":"1bd9ea6186450f9cd253ccfed281
2b1c":"":"":"":"35214bbc510430e3":0:0

AES 128 GCM Decrypt test vector #2
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_AES_256_GCM:-
1:"449d39f863e4909984b37f2e5c09ea4d4b3e9fac67bd57c299e4e1d1f084aaa3":"d8e9118f331bb5a359f0aa8882861
b72":"":"":"4ddcae0bc24d622e12bdeaac73e8d1ab7957af051d27dfaafce53aeed4cdd3f989ea25989a2f41cfb3c38dbd
841c5560b0b5ab1861b1fbcd236865d13da55b50219462e021f8a21848a64a85326031fcec8fe47a6ef4a435dd2b2fff6
37644ffcf3914ef2dfa5dd556421bfd297be150b31db039f0f2cc422b282e659e70cceb":"c595b9d99414891228c9fa5ed
b5fcce3":0:0

AES
128 GCM Decrypt test vector #3
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_AES_256_GCM:-
1:"1a1bb9122e762ecd7ff861a1d65e52607d98e7ae5bd1c3a944e443710f3b0599":"32f99ea4cbf52c2701c2252e5e6c
863d":"":"":"91b7a70c3a06c1f7f2ea584acb5dd76177ba07323c94f2e8f7cbe93fc0bb7c389c3c88e16aa53174f0fc373
bc778a6ccf91bf61b6e92c2969d3441eb17a0a835d30dcf882472a6d3cb036533b04d79f05ebfaadf221ae1c14af3f02fa
41867acfdfa35f81e8a9d11d42b9a63288c759063c0c3040c3e6ee69cf7c75f9c33fea1":"a8e29e08623a3efdbbe8b111d
e30a4":0:MBEDTLS_ERR_CIPHER_AUTH_FAILED

AES 128 GCM Decrypt test vector #4
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_AES_256_GCM:-
1:"f10965a66255f0c3515af497ccbb257a09f22ec2d57c5edae322a3e6d2d188ef":"c571ce0e911de5d883dc4a0787483
235":"91598690edf2de8b27f9bc7461a84e80811cee544f0542923898328cf157590251f0342cb81d359b5dccc5391a1
2320d1444c26f24178977dd6705c2b365dc1ece0152c42e2f0ee3162cf886ef5529f4f16a77f3bdd2aeccd405b59addf09
8521d0d38cc25f1991e11be7ecf24caedb48a2a286d2e560a38fa9001c5a228c4d1":"2867996e389e09ec0da94d42e77
b1e436b50065b09ca4adf1cd03240444ee699dbb7b3fc081a1869ca607d77d5ff9754fc3c997ff0a4ee17543a2ba77886
b88a7128bcc51d3450df58ff3a26671b02c1d213df6adb6f7e853080eb46b504517cbaea162710a9bbc2da8b552eb6b0e
0cb98e44fcab0a157312be67974678d143e":"":"6d9d3a5dbc8dce385f092fff14bfffda":0:0

AES
128 GCM Decrypt test vector #5
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_AES_256_GCM:-
1:"4103b1ddff87a508a219c808a04ad4750668688f4c2ee75b92d28d70b98a2c94":"5cea906737518c2cb901016e302
06276":"a00a196193ff07006b7df524824bd0971d63f447a3a7bb1b75c1e2d11789482c115cff677b54948d36dc4de34
200bce97be0101d88cee39b177857dd5da3cb0d2f9d6e1150f72a3bd655e0bace1d25a657ba9a7f8dff082b4460432075
afb20173da22b49beeb6a030d72ba07869ff4389fc1c28d87018d7c1a9829c21932197":"":"":"3a3a771dd5f31c977e15
4ef5c73a":0:MBEDTLS_ERR_CIPHER_AUTH_FAILED

AES
128 GCM Decrypt test vector #6
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_AES_256_GCM:-
1:"df867d1dd8a287821a54479cab6f88636d2aca30e1bf01a5dffc735e17590356":"35019826c51dd1ef07ff915d9ac4e
a96":"6517272cac85d7f38902bcb4b96a0c59c4bdc46bfefa6ebacd7f2fb1629b87ca91de2ffefc42ce3cfd34dcbf01b3f7
cadcea3f99e6addf35d36c51f2ceb1f85c1f56a04ec9c9fff60cd7fc238674992183ea3de72ef778561b906202b7b83fe65
62a0bca9c1e0a18638e8685b998b4192f5120435809ad6e93a0422d00725262":"723be39bc13adbc48c861b07753f64f
ac1ae28fc8933acba888b6538721df0a8b91c040a26522fe0dbb7335d8f63d209e89f7cde23afa9ca3c584b336d63a91e0
7fdd8808b14c3214c96a202e665bbaaa34248ff30348f3d79c9f16e66ad6c5903305acd887a89b6244eb7c2d96e18b13a
686de935bf3821444ee20f48678be5":"0375ed93f287eefe414ab2968844bd10148860c528dbf571a77aa74f98cc669a7
fc317adc9f7cf2d80dda29b19db635b30a044399f3665b6176ed669146d28f5ada03b3d32d53fe46575a8afcd37f20386
d9e36f7e090b4fefadfab7f008e02f1b5022c0eeb81d03443a276eae48c038ed173631687d2450b913b02c97243edb":"e
49beb083a9b008ae97a17e3825692f0":0:0

AES
128 GCM Decrypt test vector #7
depends_on:MBEDTLS_AES_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_AES_256_GCM:-
1:"886c77b80f5f3a21c01932685a540b23629f6d41d5574fc527227ed0bdf2e21b":"5ec506edb1890a5a63b464490450
d419":"53a17d7b69f607f08676d6f6dd4e8db08e01333a8355d8c87616e84cdf10ef5b041fc6ddc3f6a245c0f534c2b16
7064af82f45e4702a5e8dede59579fdecf6713353392433950c9b97c38d9ee515ac97d0970ccf03981954540088567a30
941bb2cca08cbed680500f8342faa7aebbc6c143e2ea57ba6b4ac1fd975dcc5d0871":"79ee27adfa9698a97d217c5010e
c807806feda37db811e398c3b82abf698aece08561fffc6c601d2691738e279eeb57e5804e1405a9913830e3ba0d7b979
213ef40d733a19497d4bb1b8b2c609a8f904e29771fa230c39a48ebb8c3376f07c8013fff6e34f10fe53988a6ec87a9296
c0a7cfba769adefe599ec6671012965973":"05b8d820c9f439d7aeae5c7da0ee25fb0dad47cc3e6f3a47e8b984e856201
546975f8214531fc3c2e504d2ac10fa49cb948596b9a8fab01b95c49d6f04d1589f93b77b899e803dd20e1f00a51c0b59

53e85be639109b14b100e35ca26d84ea629964b0db8260dfa5a150a66261bf37e79de2ec49e9f1b082a7c58ecd3d39b6c9":"ffdf56e1c1a7252b88422787536484":0:0

CAMELLIA
128 GCM Encrypt and decrypt 0 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_GCM:"CAMELLIA-128-GCM":128:0:-1

CAMELLIA 128 GCM Encrypt and decrypt 1 byte
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_GCM:"CAMELLIA-128-GCM":128:1:-1

CAMELLIA 128 GCM Encrypt and decrypt 2 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_GCM:"CAMELLIA-128-GCM":128:2:-1

CAMELLIA 128 GCM Encrypt and decrypt 7 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_GCM:"CAMELLIA-128-GCM":128:7:-1

CAMELLIA 128 GCM Encrypt and decrypt 8 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_GCM:"CAMELLIA-128-GCM":128:8:-1

CAMELLIA
128 GCM Encrypt and decrypt 9 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_GCM:"CAMELLIA-128-GCM":128:9:-1

CAMELLIA 128 GCM Encrypt and decrypt 15 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_GCM:"CAMELLIA-128-GCM":128:15:-1

CAMELLIA 128 GCM Encrypt and decrypt 16 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_GCM:"CAMELLIA-128-GCM":128:16:-1

CAMELLIA 128 GCM Encrypt and decrypt 17 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_GCM:"CAMELLIA-128-GCM":128:17:-1

CAMELLIA 128 GCM Encrypt and decrypt 31 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_GCM:"CAMELLIA-128-GCM":128:31:-1

CAMELLIA 128 GCM Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_GCM:"CAMELLIA-128-GCM":128:32:-1

CAMELLIA
128 GCM Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_GCM:"CAMELLIA-128-GCM":128:33:-1

CAMELLIA 128 GCM Encrypt and decrypt 47 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_GCM:"CAMELLIA-128-GCM":128:47:-1

CAMELLIA 128 GCM Encrypt and decrypt 48 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_GCM:"CAMELLIA-128-GCM":128:48:-1

CAMELLIA 128 GCM Encrypt and decrypt 49 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_GCM:"CAMELLIA-128-GCM":128:49:-1

CAMELLIA 128 GCM Encrypt and decrypt 0 bytes in multiple parts
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_GCM:128:0:0

CAMELLIA 128 GCM Encrypt and decrypt 1 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_GCM:128:1:0

CAMELLIA
128 GCM Encrypt and decrypt 1 bytes in multiple parts 2
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_GCM:128:0:1

CAMELLIA 128 GCM Encrypt and decrypt 16 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_GCM:128:16:0

CAMELLIA 128 GCM Encrypt and decrypt 16 bytes in multiple parts 2
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_GCM:128:0:16

CAMELLIA 128 GCM Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_GCM:128:16:6

CAMELLIA 128 GCM Encrypt and decrypt 22 bytes in multiple parts 2
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_GCM:128:0:22

CAMELLIA 128 GCM Encrypt and decrypt 32 bytes in multiple parts 1

depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_GCM:128:16:16

CAMELLIA
128 GCM Decrypt test vector #1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_CAMELLIA_128_GCM:-
1:"00000000000000000000000000000000":"00000000000000000000000000":"":"":"":"f5574acc3148dfcb9015200631024df8":0:MBEDTLS_ERR_CIPHER_AUTH_FAILED

CAMELLIA 128 GCM Decrypt test vector #2
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_CAMELLIA_128_GCM:-
1:"00000000000000000000000000000000":"00000000000000000000000000":"defe3e0b5c54c94b4f2a0f5a46f6210d":"00000000000000000000000000000000":"":"f672b94d192266c7c8c8dbb427cc989a":0:0

CAMELLIA 128 GCM Decrypt test vector #3
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_CAMELLIA_128_GCM:-
1:"feffe9928665731c6d6a8f9467308308":"cafebabefacedbaddecaf889":"d0d94a13b632f337a0cc9955b94fa020c815f903aab12f1efaf2fe9d90f729a6cccbfa986ef2ff2c33de418d9a2529091cf18fe652c1cfde13f8260614bab815":"":"":"86e318012dd8329dc9dae6a170f61b24":0:MBEDTLS_ERR_CIPHER_AUTH_FAILED

CAMELLIA
128 GCM Decrypt test vector #4
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_CAMELLIA_128_GCM:-
1:"feffe9928665731c6d6a8f9467308308":"cafebabefacedbaddecaf888":"d0d94a13b632f337a0cc9955b94fa020c815f903aab12f1efaf2fe9d90f729a6cccbfa986ef2ff2c33de418d9a2529091cf18fe652c1cfde13f82606":"d9313225f88406e5a55909c5aff5269a86a7a9531534f7da2e4c303d8a318a721c3c0c95956809532fcf0e2449a6b525b16aedf5aa0de657ba637b39":"feedfacedeadbeeffeedfacedeadbeefabaddad2":"9f458869431576ea6a095456ec6b8101":0:0

CAMELLIA 128 GCM Decrypt test vector #5
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_CAMELLIA_128_GCM:-
1:"feffe9928665731c6d6a8f9467308308":"cafebabefacedbad":"28fd7434d5cd424a5353818fc21a982460d20cf632eb1e6c4fbfca17d5abcf6a52111086162fe9570e7774c7a912aca3dfa10067ddaad40688645bdd":"":"feedfadedeadbeeffedfacedeadbeefabaddad2":"e86f8f2e730c49d536f00fb5225d28b1":0:MBEDTLS_ERR_CIPHER_AUTH_FAILED

CAMELLIA
192 GCM Encrypt and decrypt 0 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_192_GCM:"CAMELLIA-192-GCM":192:0:-1

CAMELLIA 192 GCM Encrypt and decrypt 1 byte
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_192_GCM:"CAMELLIA-192-GCM":192:1:-1

CAMELLIA 192 GCM Encrypt and decrypt 2 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_192_GCM:"CAMELLIA-192-GCM":192:2:-1

CAMELLIA 192 GCM Encrypt and decrypt 7 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_192_GCM:"CAMELLIA-192-GCM":192:7:-1

CAMELLIA 192 GCM Encrypt and decrypt 8 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_192_GCM:"CAMELLIA-192-GCM":192:8:-1

CAMELLIA 192 GCM Encrypt and decrypt 9 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_192_GCM:"CAMELLIA-192-GCM":192:9:-1

CAMELLIA 192 GCM Encrypt and decrypt
15 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_192_GCM:"CAMELLIA-192-GCM":192:15:-1

CAMELLIA 192 GCM Encrypt and decrypt 16 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_192_GCM:"CAMELLIA-192-GCM":192:16:-1

CAMELLIA 192 GCM Encrypt and decrypt 17 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_192_GCM:"CAMELLIA-192-GCM":192:17:-1

CAMELLIA 192 GCM Encrypt and decrypt 31 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_192_GCM:"CAMELLIA-192-GCM":192:31:-1

CAMELLIA 192 GCM Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_192_GCM:"CAMELLIA-192-GCM":192:32:-1

CAMELLIA 192 GCM Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_192_GCM:"CAMELLIA-192-GCM":192:33:-1

CAMELLIA 192 GCM Encrypt and decrypt 47 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_192_GCM:"CAMELLIA-192-GCM":192:47:-1

CAMELLIA
192 GCM Encrypt and decrypt 48 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C

enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_192_GCM:"CAMELLIA-192-GCM":192:48:-1

CAMELLIA 192 GCM Encrypt and decrypt 49 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_192_GCM:"CAMELLIA-192-GCM":192:49:-1

CAMELLIA 192 GCM Encrypt and decrypt 0 bytes in multiple parts
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_192_GCM:192:0:0

CAMELLIA 192 GCM Encrypt and decrypt 1 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_192_GCM:192:1:0

CAMELLIA 192 GCM Encrypt and decrypt 1 bytes in multiple parts 2
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_192_GCM:192:0:1

CAMELLIA 192 GCM Encrypt and decrypt 16 bytes
in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_192_GCM:192:16:0

CAMELLIA 192 GCM Encrypt and decrypt 16 bytes in multiple parts 2
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_192_GCM:192:0:16

CAMELLIA 192 GCM Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_192_GCM:192:16:6

CAMELLIA 192 GCM Encrypt and decrypt 22 bytes in multiple parts 2
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_192_GCM:192:0:22

CAMELLIA 192 GCM Encrypt and decrypt 32 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_192_GCM:192:16:16

CAMELLIA 192 GCM Decrypt test vector #1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_CAMELLIA_192_GCM:-
1:"000000000000000000000000000000000000000000000000":"00000000000000000000000":"":"":"":"ba9ae89f
ddce4b51131e17c4d65ce587":0:0

CAMELLIA
192 GCM Decrypt test vector #2
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C

decrypt_test_vec:MBEDTLS_CIPHER_CAMELLIA_192_GCM:-
1:"000000000000000000000000000000000000000000000000":"00000000000000000000000":"8f9c0aa2549714c
88bb2665e8af86d42":"":"":"783cff5c5aca7197320658a74279ab37":0:MBEDTLS_ERR_CIPHER_AUTH_FAILED

CAMELLIA 192 GCM Decrypt test vector #3
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_CAMELLIA_192_GCM:-
1:"feffe9928665731c6d6a8f9467308308feffe9928665731c":"cafebabefacedbaddecaf888":"0f009e88410d84ad93c9
0d55efbe20ffa855492f4dfd0fb485c4f02f536feffbb4d967729e5c67f1de0750255cc500716ba483eb3b0a2bf607af28f6
a60bb2e9":"d9313225f88406e5a55909c5aff5269a86a7a9531534f7da2e4c303d8a318a721c3c0c95956809532fcf0e2
449a6b525b16aedf5aa0de657ba637b391aafd255":"":"8d645a0b0e48d3c3b60a014157cb49b4":0:0

CAMELLIA 192 GCM Decrypt test vector #4
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_CAMELLIA_192_GCM:-
1:"feffe9928665731c6d6a8f9467308308feffe9928665731c":"cafebabefacedbaddecaf888":"0f009e88410d84ad93c9
0d55efbe20ffa855492f4dfd0fb485c4f02f536feffbb4d967729e5c67f1de0750255cc500716ba483eb3b0a2bf607af28f6
":"":"feedfacedeadbeeffeedfacedeadbeefabaddad2":"11b15bb5ab6fac0c422014e91eacbf2b":0:MBEDTLS_ERR_CI
PHER_AUTH_FAILED

CAMELLIA
192 GCM Decrypt test vector #5
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_CAMELLIA_192_GCM:-
1:"feffe9928665731c6d6a8f9467308308feffe9928665731c":"cafebabefacedbad":"678b3dcb270faa206dc5f6fbb5014
996e86d6f3e35cdcdfeb03b37b9b06ff4ff2682248823bd3c84124dc76af7bde3dd440c228b5efbc795dd80dfb6":"d931
3225f88406e5a55909c5aff5269a86a7a9531534f7da2e4c303d8a318a721c3c0c95956809532fcf0e2449a6b525b16ae
df5aa0de657ba637b39":"feedfacedeadbeeffeedfacedeadbeefabaddad2":"f876143d933214a5035ff0bb96ff650b":0:0

CAMELLIA 256 GCM Encrypt and decrypt 0 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_256_GCM:"CAMELLIA-256-GCM":256:0:-1

CAMELLIA
256 GCM Encrypt and decrypt 1 byte
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_256_GCM:"CAMELLIA-256-GCM":256:1:-1

CAMELLIA 256 GCM Encrypt and decrypt 2 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_256_GCM:"CAMELLIA-256-GCM":256:2:-1

CAMELLIA 256 GCM Encrypt and decrypt 7 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_256_GCM:"CAMELLIA-256-GCM":256:7:-1

CAMELLIA 256 GCM Encrypt and decrypt 8 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C

enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_256_GCM:"CAMELLIA-256-GCM":256:8:-1

CAMELLIA 256 GCM Encrypt and decrypt 9 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_256_GCM:"CAMELLIA-256-GCM":256:9:-1

CAMELLIA 256 GCM Encrypt and decrypt 15 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_256_GCM:"CAMELLIA-256-GCM":256:15:-1

CAMELLIA
256 GCM Encrypt and decrypt 16 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_256_GCM:"CAMELLIA-256-GCM":256:16:-1

CAMELLIA 256 GCM Encrypt and decrypt 17 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_256_GCM:"CAMELLIA-256-GCM":256:17:-1

CAMELLIA 256 GCM Encrypt and decrypt 31 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_256_GCM:"CAMELLIA-256-GCM":256:31:-1

CAMELLIA 256 GCM Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_256_GCM:"CAMELLIA-256-GCM":256:32:-1

CAMELLIA 256 GCM Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_256_GCM:"CAMELLIA-256-GCM":256:33:-1

CAMELLIA 256 GCM Encrypt and decrypt 47 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_256_GCM:"CAMELLIA-256-GCM":256:47:-1

CAMELLIA
256 GCM Encrypt and decrypt 48 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_256_GCM:"CAMELLIA-256-GCM":256:48:-1

CAMELLIA 256 GCM Encrypt and decrypt 49 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_256_GCM:"CAMELLIA-256-GCM":256:49:-1

CAMELLIA 256 GCM Encrypt and decrypt 0 bytes in multiple parts
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_256_GCM:256:0:0

CAMELLIA 256 GCM Encrypt and decrypt 1 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_256_GCM:256:1:0

CAMELLIA 256 GCM Encrypt and decrypt 1 bytes in multiple parts 2
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_256_GCM:256:0:1

CAMELLIA 256 GCM Encrypt and decrypt 16 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_256_GCM:256:16:0

CAMELLIA
256 GCM Encrypt and decrypt 16 bytes in multiple parts 2
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_256_GCM:256:0:16

CAMELLIA 256 GCM Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_256_GCM:256:16:6

CAMELLIA 256 GCM Encrypt and decrypt 22 bytes in multiple parts 2
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_256_GCM:256:0:22

CAMELLIA 256 GCM Encrypt and decrypt 32 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_256_GCM:256:16:16

CAMELLIA 256 GCM Decrypt test vector #1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_CAMELLIA_256_GCM:-
1:"0000000000000000000000000000000000000000000000000000000000000001":"00000000000000000000000"
:"":"":"":"9cdb269b5d293bc5db9c55b057d9b591":0:MBEDTLS_ERR_CIPHER_AUTH_FAILED

CAMELLIA
256 GCM Decrypt test vector #2
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_CAMELLIA_256_GCM:-
1:"0000000000000000000000000000000000000000000000000000000000000000":"00000000000000000000000"
:"3d4b2cde666761ba5dfb305178e667fb":"00000000000000000000000000000000":"":"284b63bb143c40ce100fb4d
ea6bb617b":0:0

CAMELLIA 256 GCM Decrypt test vector #3
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_CAMELLIA_256_GCM:-
1:"feffe9928665731c6d6a8f9467308308feffe9928665731c6d6a8f9467308308":"cafebabefacedbaddecaf888":"ad14
2c11579dd95e41f3c1f324dabc255864d920f1b65759d8f560d4949d447758dfdcf77aa9f62581c7ff572a037f810cb1a9

c4b3ca6ed638179b776549e092":"":"":"c912686270a2b9966415fca3be75c468":0:MBEDTLS_ERR_CIPHER_AUTH_FAILED

CAMELLIA 256 GCM Decrypt test vector #4
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_CAMELLIA_256_GCM:-
1:"feffe9928665731c6d6a8f9467308308feffe9928665731c6d6a8f9467308308":"cafebabefacedbaddecaf888":"ad142c11579dd95e41f3c1f324dabc255864d920f1b65759d8f560d4948d447758dfdcf77aa9f62581c7ff572a037f810cb1a9c4b3ca6ed638179b77":"d9313225f88406e5a55909c5aff5269a86a7a9531534f7da2e4c303d8a318a721c3c0c95956809532fcf0e2449a6b525b16aedf5aa0de657ba637b39":"feedfacedeadbeeffeedfacedeadbeefabaddad2":"4e4b178d8fe26fdc95e2e7246dd94bec":0:0

CAMELLIA
256 GCM Decrypt test vector #5
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_GCM_C
decrypt_test_vec:MBEDTLS_CIPHER_CAMELLIA_256_GCM:-
1:"feffe9928665731c6d6a8f9467308308feffe9928665731c6d6a8f9467308308":"cafebabefacedbad":"6ca95fbb7d16577a9ef2fded94dc85b5d40c629f6bef2c649888e3cbb0ededc7810c04b12c2983bbbbc482e16e45c9215ae12c15c55f2f4809d06652":"":"feedfacedeadbeeffeedfacedeadbeefabaddad2":"e6472b8ebd331bfcc7c0fa63ce094462":0:MBEDTLS_ERR_CIPHER_AUTH_FAILED
-----BEGIN CERTIFICATE-----
MIICHzCCAaWgAwIBAgIBFTAKBggqhkjOPQQDBDA+MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EwHhcN
MTMwOTI0MTYyMTI3WhcNMjMwOTIyMTYyMTI3WjA0MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxEjAQBgNVBAMTCWxvY2FsaG9zdDBZMBMGByqGSM49AgEG
CCqGSM49AwEHA0IABDfMVtl2CR5acj7HWS3/IG7ufPkGkXTQrRS192giWWKSTuUA
2CMR/+ov0jRdXRa9iojCa3cNVc2KKg76Aci07f+jgZ0wgZowCQYDVR0TBAIwADAd
BgNVHQ4EFgQUUGlj9QH2deCAQzlZX+MY0anE74wbgYDVR0jBGcwZYAUnW0gJEkB
PyvLeLUZvH4kydv7NnyhQqRAMD4xCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQb2xh
clNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBFQyBDQYIJAMFD4n5iQ8zoMAoG
CCqGSM49BAMEA2gAMGUCMFPL2OI8arcbRlKAbRb/YfGibo4Mwts8KX3fOuRCbXEn
pDWeb82kBqfXwzPJwamFOwIxAPGzyhWrxn0qEynWV5nzFK02PYBnYFgClISyyudH
HJGHtbEVRc5JA8ALnggaLVpuvg==
-----END CERTIFICATE-----
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>

```
    <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
    <Configuration>Release</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
</ItemGroup>
<ItemGroup>
  <ClCompile Include="..\..\programs\pkey\dh_server.c" />
</ItemGroup>
<ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">

    <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
</ItemGroup>
<PropertyGroup Label="Globals">
  <ProjectGuid>{8D91B804-E2CE-142D-8E06-FBB037ED1F65}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>dh_server</RootNamespace>
</PropertyGroup>
<Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
    <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
</PropertyGroup>
<Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
<ImportGroup Label="ExtensionSettings">
</ImportGroup>
```

```
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
 />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
    <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
   <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <LinkIncremental>false</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
   <LinkIncremental>false</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <ClCompile>
     <PrecompiledHeader>
     </PrecompiledHeader>
     <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
      <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
     <SubSystem>Console</SubSystem>
     <GenerateDebugInformation>true</GenerateDebugInformation>
     <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
```

2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
<AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
</Link>
<ProjectReference>
<LinkLibraryDependencies>false</LinkLibraryDependencies>
</ProjectReference>
</ItemDefinitionGroup>
<ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
<ClCompile>
<PrecompiledHeader>
</PrecompiledHeader>
<WarningLevel>Level3</WarningLevel>
<Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
<AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
</ClCompile>
<Link>
<SubSystem>Console</SubSystem>
<GenerateDebugInformation>true</GenerateDebugInformation>
<ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
<AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
</Link>
<ProjectReference>
<LinkLibraryDependencies>false</LinkLibraryDependencies>
</ProjectReference>
</ItemDefinitionGroup>
<ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
<ClCompile>
<WarningLevel>Level3</WarningLevel>
<PrecompiledHeader>
</PrecompiledHeader>
<Optimization>MaxSpeed</Optimization>
<FunctionLevelLinking>true</FunctionLevelLinking>
<IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
<AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
</ClCompile>
<Link>
<SubSystem>Console</SubSystem>
<GenerateDebugInformation>true</GenerateDebugInformation>
<EnableCOMDATFolding>true</EnableCOMDATFolding>
<OptimizeReferences>true</OptimizeReferences>
<AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3

```
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
    </Link>
  </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
    <ClCompile>
      <WarningLevel>Level3</WarningLevel>
      <PrecompiledHeader>
      </PrecompiledHeader>
      <Optimization>MaxSpeed</Optimization>
      <FunctionLevelLinking>true</FunctionLevelLinking>
      <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
      <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
    </ClCompile>
    <Link>
      <SubSystem>Console</SubSystem>
      <GenerateDebugInformation>true</GenerateDebugInformation>
      <EnableCOMDATFolding>true</EnableCOMDATFolding>
      <OptimizeReferences>true</OptimizeReferences>
      <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
      <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
    </Link>
  </ItemDefinitionGroup>
  <Import
  Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
  <ImportGroup Label="ExtensionTargets">
  </ImportGroup>
</Project>
-----BEGIN PUBLIC KEY-----
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEd3Jlb4FLOZJ51eHxeB+sbwmaPFyh
sONTUYNLCLZeC1clkM2vj3aTYbzzSs/BHl4HToQmvd4Evm5lOUVElhfeRQ==
-----END PUBLIC KEY-----
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
  <ItemGroup Label="ProjectConfigurations">
    <ProjectConfiguration Include="Debug|Win32">
      <Configuration>Debug</Configuration>
      <Platform>Win32</Platform>
    </ProjectConfiguration>
    <ProjectConfiguration Include="Debug|x64">
      <Configuration>Debug</Configuration>
      <Platform>x64</Platform>
    </ProjectConfiguration>
    <ProjectConfiguration Include="Release|Win32">
      <Configuration>Release</Configuration>
      <Platform>Win32</Platform>
```

```
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
    <Configuration>Release</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
</ItemGroup>
<ItemGroup>
  <ClCompile Include="..\..\programs\hash\generic_sum.c" />
</ItemGroup>
<ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">
    <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
</ItemGroup>
<PropertyGroup Label="Globals">
  <ProjectGuid>{D071CCF7-ACA0-21F8-D382-52A759AEA261}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>generic_sum</RootNamespace>
</PropertyGroup>
<Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
</PropertyGroup>
<Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
<ImportGroup Label="ExtensionSettings">
</ImportGroup>
<ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
```

```
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
 />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
    <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
   <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <LinkIncremental>false</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
   <LinkIncremental>false</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <ClCompile>
     <PrecompiledHeader>
     </PrecompiledHeader>
     <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
      <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
     <SubSystem>Console</SubSystem>
     <GenerateDebugInformation>true</GenerateDebugInformation>
     <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
```

```
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
```

```
  </Link>
 </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
 <Import
 Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQI4W7G1sVqHJMCAggA
MBQGCCqGSIb3DQMHBAjXOQ/kHb9EVASCBMg68SwrdD/DLeKcPtCkE36wHvrK6wi7
CjwFv2U/gIfNCUNXBZPI4G7voL1XOLJ8h0WWqlEraHo7zYWI5Ky98SI6wOpDGDzo
URvavOVT3Ry/QfLtt0GZvELmJb6qO2AcL1qIDULx4xXqb3rI29xR/xVaCkB8CGSe
JxU+1TbJJG0UdVDm28dhO8J4qgBpj9N6M/e8K1TIu8ty6IkFPFumTN9zMV9VXRIo
Ajr1RDIiFXCZ4ayEnja2RIZwi89rn/iC/QzfsqQFr5axw58wz+0/EfD/i79gKoOX
jKBEwWN44LsxJW/ucy3pm7xRurwZvOQZIeZcecVVecAaHmCRFfq+VpSnU5iDZEDL
0GU+CKXW+zDnuIfUc/lx7LWjFyqR12OviS2CdrkaTKSVBAEYCFQdGPCp51WoZMnE
uaKkLp0y58e5J0mHx4kmk2saAacdO/YolHjkh5zNe1Z+sORwPEo4ruZY/+wem/TG
KFQsVjH/jAsyQFsyXaOrQ4QyOwxw52Vz6b7vrffaTdnKlyvJTvebEbhNiNmt2Ni+
wac/1VcedkMpUrNmpJyal6lzWrVQmW1Q9qBinxHeGnNHk2QWTGZCQCClxDTfPoE1
HC85cD4h91eBV4fiQm/ML/WmaGAQGUiTlX5vESJG1pKYXGqv1cr1pj+MTjqfjApl
KOj93yAvx4ss42onWe9DPOBojSMuIzEVZOeq7mt7QeNpN9unjsDVrvq/fmsvIBb0
t5HFVX4JlZoF2sfrwP0jEkyHxlk0pZZc5rbwtVI601MolDzjTNBcYbUB0IUlIj9f
mM35IAFWZtrXXv3k5ZRFQU2jB7DFP9zHWsai7quhhduvt498rNxiWu7YlAQfhaU/
wVK+3Fca7AGrlQ8YmzV0uOwoTMvKbLNwiiIG6QsgWRhmOIwHdNlRvhaZl6ybRLty
ppMaqlOgDu88/8SMCce8yBderXW/0QxCZjQ3gEDufqxjC2IelOfEbChMLIs6p+9B
qaPtji3TxOscQZMD9g4jYXUawHSq55B/MegD5sfvTl3ql+qsQnleXDUz2gJ+MBlH
Qp6HZMs2woAbvFyxAXSUeKAOZrnW1TmRNmj6SwtE9aPmMwSYxZtTukesl+CpzEqi
BdBZia3Yxu9Z5694Cg1eXoPIir6u6svZA5OIpEIUDIUPnMmG9pjxQ1xK40vyjdMZ
```

+9uAVdGX118nuwZ6Al4bfrPOOmwII2X1xmfFGG3rbVHVD9dIGJ1HGWPZio4F/eai
kfSYHr0410JRAOvd9G4vrH6rq/zE5QcLCmXyH5W9vF3RJDAK4ArcaLF5RPY8slEJ
NcZ7XTcKUc/Tg6VCMo3agozuzrxKCX5x6rvn0COYgdU3ozTO72dJlFQY2KpJP0n2
RWWjdl2r7XYVRoQJd5XaZ3/mgJ7FtL42Rh6+vjEJLezWgUTo3B4Z0WG8WIp4wfAw
d4qbAa4lVWtP++HZvIqOPaL+nZgFS22ygtoIVyYDj7lcqH9cdMsaMrZFAxisVQK2
z2DnysfLg4dkdDuJjFUI07QUPwqjfRVKC8Mec45j9zrpuzu82zQ8Fub7ldtECsby
oq0smBG1vd+ozMPnr3yvU7X7jaaM4toW+dG3OQxnUO2GyB/BAEamOB4CWWbKSfy1
tfM=
-----END
ENCRYPTED PRIVATE KEY-----
CCM self test
mbedtls_ccm_self_test:

CCM init #1 AES-128: OK
depends_on:MBEDTLS_AES_C
mbedtls_ccm_setkey:MBEDTLS_CIPHER_ID_AES:128:0

CCM init #2 CAMELLIA-256: OK
depends_on:MBEDTLS_CAMELLIA_C
mbedtls_ccm_setkey:MBEDTLS_CIPHER_ID_CAMELLIA:256:0

CCM init #3 AES-224: bad key size
depends_on:MBEDTLS_AES_C
mbedtls_ccm_setkey:MBEDTLS_CIPHER_ID_AES:224:MBEDTLS_ERR_CCM_BAD_INPUT

CCM init #4 BLOWFISH-128: bad block size
depends_on:MBEDTLS_BLOWFISH_C
mbedtls_ccm_setkey:MBEDTLS_CIPHER_ID_BLOWFISH:128:MBEDTLS_ERR_CCM_BAD_INPUT

CCM lengths #1 all OK
ccm_lengths:5:10:5:8:0

CCM lengths #2 nonce too short
ccm_lengths:5:6:5:8:MBEDTLS_ERR_CCM_BAD_INPUT

CCM lengths #3 nonce too long
ccm_lengths:5:14:5:8:MBEDTLS_ERR_CCM_BAD_INPUT

CCM lengths #4 tag too short
ccm_lengths:5:10:5:2:MBEDTLS_ERR_CCM_BAD_INPUT

CCM lengths #5 tag too long
ccm_lengths:5:10:5:18:MBEDTLS_ERR_CCM_BAD_INPUT

CCM lengths #6 tag length not even
ccm_lengths:5:10:5:7:MBEDTLS_ERR_CCM_BAD_INPUT

CCM lenghts #7 AD too long (2^16 - 2^8

+ 1)
ccm_lengths:5:10:65281:8:MBEDTLS_ERR_CCM_BAD_INPUT

CCM lengths #8 msg too long for this IV length (2^16, q = 2)
ccm_lengths:65536:13:5:8:MBEDTLS_ERR_CCM_BAD_INPUT

CCM encrypt and tag RFC 3610 #1
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF":"08090A0B0C0D0E0F101112131415161718191A1B1C1D1E":"00000003020100A0A1A2A3A4A5":"0001020304050607":"588C979A61C663D2F066D0C2C0F989806D5F6B61DAC38417E8D12CFDF926E0"

CCM encrypt and tag RFC 3610 #2
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF":"08090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F":"00000004030201A0A1A2A3A4A5":"0001020304050607":"72C91A36E135F8CF291CA894085C87E3CC15C439C9E43A3BA091D56E10400916"

CCM encrypt and tag RFC 3610 #3
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF":"08090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F20":"00000005040302A0A1A2A3A4A5":"0001020304050607":"51B1E5F44A197D1DA46B0F8E2D282AE871E838BB64DA8596574ADAA76FBD9FB0C5"

CCM
encrypt and tag RFC 3610 #4
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF":"0C0D0E0F101112131415161718191A1B1C1D1E":"00000006050403A0A1A2A3A4A5":"000102030405060708090A0B":"A28C6865939A9A79FAAA5C4C2A9D4A91CDAC8C96C861B9C9E61EF1"

CCM encrypt and tag RFC 3610 #5
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF":"0C0D0E0F101112131415161718191A1B1C1D1E1F":"00000007060504A0A1A2A3A4A5":"0001020304050607 08090A0B":"DCF1FB7B5D9E23FB9D4E131253658AD86EBDCA3E51E83F077D9C2D93"

CCM encrypt and tag RFC 3610 #6
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF":"0C0D0E0F101112131415161718191A1B1C1D1E1F20":"00000008070605A0A1A2A3A4A5":"0001020304050607 08090A0B":"6FC1B011F006568B5171A42D953D469B2570A4BD87405A0443AC91CB94"

CCM
encrypt and tag RFC 3610 #7
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF":"08090A0B0C0D0E0F101112131415161718191A1B1C1D1E":"00000009080706A0A1A2A3A4A5":"0001020304

050607":"0135D1B2C95F41D5D1D4FEC185D166B8094E999DFED96C048C56602C97ACBB7490"

CCM encrypt and tag RFC 3610 #8
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF":"08090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F":"0000000A090807A0A1A2A3A4A5":"0001020304050607":"7B75399AC0831DD2F0BBD75879A2FD8F6CAE6B6CD9B7DB24C17B4433F434963F34B4"

CCM encrypt and tag RFC 3610 #9
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF":"08090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F20":"0000000B0A0908A0A1A2A3A4A5":"0001020304050607":"82531A60CC24945A4B8279181AB5C84DF21CE7F9B73F42E197EA9C07E56B5EB17E5F4E"

CCM encrypt and tag RFC 3610 #10
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF":"0C0D0E0F101112131415161718191A1B1C1D1E":"0000000C0B0A09A0A1A2A3A4A5":"00010203040506078090A0B":"07342594157785152B074098330ABB141B947B566AA9406B4D999988DD"

CCM
encrypt and tag RFC 3610 #11
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF":"0C0D0E0F101112131415161718191A1B1C1D1E1F":"0000000D0C0B0AA0A1A2A3A4A5":"000102030405060708090A0B":"676BB20380B0E301E8AB79590A396DA78B834934F53AA2E9107A8B6C022C"

CCM encrypt and tag RFC 3610 #12
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF":"0C0D0E0F101112131415161718191A1B1C1D1E1F20":"0000000E0D0C0BA0A1A2A3A4A5":"0001020304050607080 90A0B":"C0FFA0D6F05BDB67F24D43A4338D2AA4BED7B20E43CD1AA31662E7AD65D6DB"

CCM encrypt and tag RFC 3610 #13
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"D7828D13B2B0BDC325A76236DF93CC6B":"08E8CF97D820EA258460E96AD9CF5289054D895CEAC47C":"00412B4EA9CDBE3C9696766CFA":"0BE1A88BACE018B1":"4CB97F86A2A4689A877947AB8091EF5386A6FFBDD080F8E78CF7CB0CDDD7B3"

CCM
encrypt and tag RFC 3610 #14
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"D7828D13B2B0BDC325A76236DF93CC6B":"9020EA6F91BDD85AFA0039BA4BAFF9BFB79C7028949CD0EC":"0033568EF7B2633C9696766CFA":"63018F76DC8A1BCB":"4CCB1E7CA981BEFAA0726C55D378061298C85C92814ABC33C52EE81D7D77C08A"

CCM encrypt and tag RFC 3610 #15
depends_on:MBEDTLS_AES_C

mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"D7828D13B2B0BDC325A76236DF93CC6B":"B916E0EACC1C00D7DCEC68EC0B3BBB1A02DE8A2D1AA346132E":"00103FE41336713C9696766CFA":"AA6CFA36CAE86B40":"B1D23A2220DDC0AC900D9AA03C61FCF4A559A4417767089708A776796EDB723506"

CCM encrypt and tag RFC 3610 #16
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"D7828D13B2B0BDC325A76236DF93CC6B":"12DAAC5630EFA5396F770CE1A66B21F7B2101C":"00764C63B8058E3C9696766CFA":"D0D0735C531E1BECF049C244":"14D253C3967B70609B7CBB7C499160283245269A6F49975BCADEAF"

CCM
encrypt and tag RFC 3610 #17
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"D7828D13B2B0BDC325A76236DF93CC6B":"E88B6A46C78D63E52EB8C546EFB5DE6F75E9CC0D":"00F8B678094E3B3C9696766CFA":"77B60F011C03E1525899BCAE":"5545FF1A085EE2EFBF52B2E04BEE1E2336C73E3F762C0C7744FE7E3C"

CCM encrypt and tag RFC 3610 #18
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"D7828D13B2B0BDC325A76236DF93CC6B":"6435ACBAFB11A82E2F071D7CA4A5EBD93A803BA87F":"00D560912D3F703C9696766CFA":"CD9044D2B71FDB8120EA60C0":"009769ECABDF48625594C59251E6035722675E04C847099E5AE0704551"

CCM encrypt and tag RFC 3610 #19
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"D7828D13B2B0BDC325A76236DF93CC6B":"8A19B950BCF71A018E5E6701C91787659809D67DBEDD18":"0042FFF8F1951C3C9696766CFA":"D85BC7E69F944FB8":"BC218DAA947427B6DB386A99AC1AEF23ADE0B52939CB6A637CF9BEC2408897C6BA"

CCM
encrypt and tag RFC 3610 #20
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"D7828D13B2B0BDC325A76236DF93CC6B":"1761433C37C5A35FC1F39F406302EB907C6163BE38C98437":"00920F40E56CDC3C9696766CFA":"74A0EBC9069F5B37":"5810E6FD25874022E80361A478E3E9CF484AB04F447EFFF6F0A477CC2FC9BF548944"

CCM encrypt and tag RFC 3610 #21
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"D7828D13B2B0BDC325A76236DF93CC6B":"A434A8E58500C6E41530538862D686EA9E81301B5AE4226BFA":"0027CA0C7120BC3C9696766CFA":"44A3AA3AAE6475CA":"F2BEED7BC5098E83FEB5B31608F8E29C38819A89C8E776F1544D4151A4ED3A8B87B9CE"

CCM encrypt and tag RFC 3610 #22
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"D7828D13B2B0BDC325A76236DF93CC6B":"B96B49E21D621741632875DB7F6C9243D2D7C2":"005B8CCBCD9AF83C9696766CFA":"EC46BB63B02520C33C49FD70":"31D750A09DA3ED7FDDD49A2032AABF17EC8EBF7D22C8088C666BE5C197"

CCM encrypt and tag RFC 3610 #23
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"D7828D13B2B0BDC325A76236DF93CC6B":"E2FCFBB880442C731BF95167C8FFD7895E337076":"003EBE94044B9A3C9696766CFA":"47A65AC78B3D594227E85E71":"E882F1DBD38CE3EDA7C23F04DD65071EB41342ACDF7E00DCCEC7AE52987D"

CCM
encrypt and tag RFC 3610 #24
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"D7828D13B2B0BDC325A76236DF93CC6B":"ABF21C0B02FEB88F856DF4A37381BCE3CC128517D4":"008D493B30AE8B3C9696766CFA":"6E37A6EF546D955D34AB6059":"F32905B88A641B04B9C9FFB58CC390900F3DA12AB16DCE9E82EFA16DA62059"

CCM encrypt and tag NIST VTT AES-128 #1 (P=24, N=13, A=32, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"43b1a6bc8d0d22d6d1ca95c18593cca5":"a2b381c7d1545c408fe29817a21dc435a154c87256346b05":"9882578e750b9682c6ca7f8f86":"2084f3861c9ad0ccee7c63a7e05aece5db8b34bd8724cc06b4ca99a7f9c4914f":"cc69ed76985e0ed4c8365a72775e5a19bfccc71aeb116c85a8c74677"

CCM encrypt and tag NIST VTT AES-128 #2 (P=24, N=13, A=32, T=6)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"44e89189b815b4649c4e9b38c4275a5a":"8db6ae1eb959963931d1c5224f29ef50019d2b0db7f5f76f":"374c83e94384061ac01963f88d":"cd149d17dba7ec50000b8c5390d114697fafb61025301f4e3eaa9f4535718a08":"df952dce0f843374d33da94c969eff07b7bc2418ca9ee01e32bc2ffa8600"

CCM
encrypt and tag NIST VTT AES-128 #3 (P=24, N=13, A=32, T=8)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"368f35a1f80eaaacd6bb136609389727":"1cccd55825316a94c5979e049310d1d717cdfb7624289dac":"842a8445847502ea77363a16b6":"34396dfcfa6f742aea7040976bd596497a7a6fa4fb85ee8e4ca394d02095b7bf":"1a58094f0e8c6035a5584bfa8d1009c5f78fd2ca487ff222f6d1d897d6051618"

CCM encrypt and tag NIST VTT AES-128 #4 (P=24, N=13, A=32, T=10)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"996a09a652fa6c82eae8be7886d7e75e":"84cdd7380f47524b86168ed95386faa402831f22045183d0":"a8b3eb68f205a46d8f632c3367":"c71620d0477c8137b77ec5c72ced4df3a1e987fd9af6b5b10853f0526d876cd5":"a7fbf9dd1b099ed3acf6bcbd0b6f7cae57bee99f9d084f826d86e69c07f053d1a607"

CCM
encrypt and tag NIST VTT AES-128 #5 (P=24, N=13, A=32, T=12)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"3ee186594f110fb788a8bf8aa8be5d4a":"d71864877f2578db092daba2d6a1f9f4698a9c356c7830a1":"44f705d52acf27b7f17196aa9b":"2c16724296ff85e079627be3053ea95adf35722c21886baba343bd6c79b5cb57":"b4dd74e7a0cc51aea45dfb401a41d5822c96901a83247ea0d6965f5aa6e31302a9cc2b36"

CCM encrypt and tag NIST VTT AES-128 #6 (P=24, N=13, A=32, T=14)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"7b2d52a5186d912cf6b83ace7740ceda":"ea384b081f60bb450808e0c20dc2914ae14a320612c3e1e8":"f47be3a2b019d1beededf5b80c":"76cf3522aff97a44b4edd0eef3b81e3ab3cd1ccc93a767a133afd508315f05ed":"79070f33114a980dfd48215051e224dfd01471ac293242afddb36e37da1ee8a88a77d7f12cc6"

CCM encrypt and tag NIST VTT AES-128 #7 (P=24, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"4189351b5caea375a0299e81c621bf43":"4535d12b4377928a7c0a61c9f825a48671ea05910748c8ef":"48c0906930561e0ab0ef4cd972":"40a27c1d1e23ea3dbe8056b2774861a4a201cce49f19997d19206d8c8a343951":"26c56961c035a7e452cce61bc6ee220d77b3f94d18fd10b6d80e8bf80f4a46cab06d4313f0db9be9"

CCM
encrypt and tag NIST VTT AES-192 #1 (P=24, N=13, A=32, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"11fd45743d946e6d37341fec49947e8c70482494a8f07fcc":"ee7e6075ba52846de5d6254959a18affc4faf59c8ef63489":"c6aeebcb146cfafaae66f78aab":"7dc8c52144a7cb65b3e5a846e8fd7eae37bf6996c299b56e49144ebf43a1770f":"137d9da59baf5cbfd46620c5f298fc766de10ac68e774edf1f2c5bad"

CCM encrypt and tag NIST VTT AES-192 #2 (P=24, N=13, A=32, T=6)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"146a163bbf10746e7c1201546ba46de769be23f9d7cc2c80":"473b6600559aefb67f7976f0a5cc744fb456efd86f615648":"f5827e51707d8d64bb522985bb":"599b12ebd3347a5ad098772c44c49eed954ec27c3ba6206d899ddaabca23a762":"26d2be30e171439d54a0fec291c6024d1de09d61b44f53258ba1360406f9"

CCM
encrypt and tag NIST VTT AES-192 #3 (P=24, N=13, A=32, T=8)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"bdf277af2226f03ec1a0ba7a8532ade6aea9b3d519fe2d38":"0ff89eff92a530b66684cd75a39481e7e069a7d05e89b692":"cc3c596be884e7caed503315c0":"4d6546167b3ed55f01c62bd384e02e1039c0d67ef7abe33291fecb136272f73b":"6ef66a52c866bd5df20ec5096de92167ad83cab0e095ad0c778a299f1224f10c"

CCM encrypt and tag NIST VTT AES-192 #4 (P=24, N=13, A=32, T=10)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"62f8eba1c2c5f66215493a6fa6ae007aae5be92f7880336a":"f5522e3405d9b77cbf3257db2b9675e618e8744a0ee03f0f":"15769753f503aa324f4b0e8ee0":"1bc05440ee3e34d0f25e90ca1ecbb555d0fb92b311621d171be6f2b719923d23":"b9103942dbbb93e15086751c9bb0a3d33112b55f95b7d4f32ff0bb90a8879812683f"

CCM encrypt and tag NIST VTT AES-192 #5 (P=24, N=13, A=32, T=12)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"5a5667197f46b8027980d0a3166c0a419713d4df06

29a860":"d0e4024d6e33daafc011fe463545ed20f172872f6f33cefa":"6236b01079d180fce156fbaab4":"29bdf65b293
94d363d5243d4249bad087520f8d733a763daa1356be458d487e5":"479f3d408bfa00d1cd1c8bf11a167ce7ae4bcdb01
1f04e38733013b8ebe5e92b1917640c"

CCM
encrypt and tag NIST VTT AES-192 #6 (P=24, N=13, A=32, T=14)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"d2d4482ea8e98c1cf309671895a16610152ce28343
4bca38":"78168e5cc3cddf4b90d5bc11613465030903e0196f1fe443":"6ee177d48f59bd37045ec03731":"9ef2d0d556
d05cf9d1ee9dab9b322a389c75cd4e9dee2c0d08eea961efce8690":"e2324a6d5643dfc8aea8c08cbbc245494a3dcbcb8
00c797c3abcdb0563978785bf7fd71c6c1f"

CCM encrypt and tag NIST VTT AES-192 #7 (P=24, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"a7177fd129674c6c91c1c89f4408139afe187026b81
14893":"2cea0f7304860a4f40a28c8b890db60f3891b9982478495e":"31bb28f0e1e63c36ca3959dd18":"2529a83466
8187213f5342a1f3deea0dc2765478c7d71c9c21b9eb1351a5f6cb":"5bb7aa6ab9c02a5712d62343fbe61f774e598d6b8
7545612380ea23dcffc9574f672bca92e306411"

CCM
encrypt and tag NIST VTT AES-256 #1 (P=24, N=13, A=32, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"9074b1ae4ca3342fe5bf6f14bcf2f27904f0b15179d9
5a654f61e699692e6f71":"239029f150bccbd67edbb67f8ae456b4ea066a4beee065f9":"2e1e0132468500d4bd478625
63":"3c5f5404370abdcb1edde99de60d0682c600b034e063b7d3237723da70ab7552":"9c8d5dd227fd9f81237601830
afee4f0115636c8e5d5fd743cb9afed"

CCM encrypt and tag NIST VTT AES-256 #2 (P=24, N=13, A=32, T=6)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"8596a69890b0e47d43aeeca54b52029331da06fae6
3aa3249faaca94e2605feb":"f0b065da6ecb9ddcab855152d3b4155037adfa758ba96070":"20442e1c3f3c88919c39978
b78":"4e0d3aa502bd03fe1761b167c4e0df1d228301d3ebaa4a0281becd813266e255":"d6a0f377f7c1b14dcdba729ca
e5271b027e71cc7850173ec265867a29eb3"

CCM
encrypt and tag NIST VTT AES-256 #3 (P=24, N=13, A=32, T=8)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"bae73483de27b581a7c13f178a6d7bda168c1b4a1c
b9180512a13e3ab914eb61":"28ef408d57930086011b167ac04b866e5b58fe6690a0b9c3":"daf54faef6e4fc7867624b7
6f2":"7022eaa52c9da821da72d2edd98f6b91dfe474999b75b34699aeb38465f70c1c":"356367c6cee4453658418d951
7f7c6faddcd7c65aef460138cf050f48c505151"

CCM encrypt and tag NIST VTT AES-256 #4 (P=24, N=13, A=32, T=10)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"d5b321b0ac2fedce0933d57d12195c7b9941f4caa95
529125ed21c41fac43374":"6aa6ea668df60b0db85592d0a819c9df9e1099916272aafb":"b35fb2262edfa14938a0fba0
3e":"ba762bbda601d711e2dfc9dbe3003d39df1043ca845612b8e9dc9ff5c5d06ec4":"97027de5effd82c58f8dbfb909d
7696fbe2d54916262912001a4d765bc1c95c90a95"

CCM encrypt and tag NIST VTT AES-256 #5 (P=24, N=13, A=32, T=12)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"7f4af6765cad1d511db07e33aaafd57646ec279db629048aa6770af24849aa0d":"7ebef26bf4ecf6f0ebb2eb860edbf900f27b75b4a6340fdb":"dde2a362ce81b2b6913abc3095":"404f5df97ece7431987bc098cce994fc3c063b519ffa47b0365226a0015ef695":"353022db9c568bd7183a13c40b1ba30fcc768c54264aa2cd2927a053c9244d3217a7ad05"

CCM
encrypt and tag NIST VTT AES-256 #6 (P=24, N=13, A=32, T=14)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"5c8b59d3e7986c277d5ad51e4a2233251076809ebf59463f47cd10b4aa951f8c":"138ee53b1914d3322c2dd0a4e02faab2236555131d5eea08":"21ff892b743d661189e205c7f3":"f1e0af185180d2eb63e50e37ba692647cac2c6a149d70c81dbd34685ed78feaa":"5b2f3026f30fdd50accc40ddd093b7997f23d7c6d3c8bc425f82c828413643b8794494cb5236"

CCM encrypt and tag NIST VTT AES-256 #7 (P=24, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"60823b64e0b2da3a7eb772bd5941c534e6ff94ea96b564e2b38f82c78bb54522":"a8be794613835c4366e75817d228438f011a2ec8a86f9797":"48526f1bffc97dd65e42906983":"fab62b3e5deda7a9c1128663cc81c44b74ab1bfe70bc1c9dec7c7fd08173b80a":"cc3efe04d84a4ec5cb6a6c28dc2c2d386a359d9550dbdec963ddd56464aed6d0613159d1aa181dcb"

CCM
encrypt and tag NIST VPT AES-128 #1 (P=0, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"2ebf60f0969013a54a3dedb19d20f6c8":"":"1de8c5e21f9db33123ff870add":"e1de6c6119d7db471136285d10b47a450221b16978569190ef6a22b055295603":"0ead29ef205fbb86d11abe5ed704b880"

CCM encrypt and tag NIST VPT AES-128 #2 (P=1, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"6ae7a8e907b8720f4b0d5507c1d0dc41":"0e":"7f18ad442e536a0159e7aa8c0f":"9c9b0f11e020c6512a63dfa1a5ec8df8bd8e2ad83cf87b80b38635621c5dc0d7":"4c201784bdab19e255787fecd02000c49d"

CCM encrypt and tag NIST VPT AES-128 #3 (P=2, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"3d746ae6cac5cefd01f021c0bbf4bc3c":"4360":"597b3614ff9cd567afd1aad4e5":"90446190e1ff5e48e8a09d692b217de3ad0ab4a670e7f1b437f9c07a902cad60":"e38fdb77c1f8bbac2903a2ec7bc0f9c5654d"

CCM
encrypt and tag NIST VPT AES-128 #4 (P=3, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"3e4fa1c6f8b00f1296956735ee86e310":"3a6734":"c6a170936568651020edfe15df":"00d57896da2435a4271afb9c98f61a650e63a4955357c47d073c5165dd4ea318":"384be657bfc5f385b179be7333eb3f57df546b"

CCM encrypt and tag NIST VPT AES-128 #5 (P=4, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"7ccbb8557f6e08f436d0957d4bbe7fdf":"4cabeb02":"bb8e2ef2ed9484f9021cda7073":"fba1d18a74a3bb38671ab2842ffaa434cd572a0b45320e4145930b3008d8d350":"32501f4235c4dd96e83d5ab4c3c31c523453c317"

CCM encrypt and tag NIST VPT AES-128 #6 (P=5, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"3725c7905bfaca415908c617b78f8dee":"f5499a7082":"c98ec4473e051a4d4ac56fd082":"11bc87f1c2d2076ba47c5cb530dd6c2a224f7a0f7f554e23d7d29077c7787680":"e378b776242066751af249d521c6eaebdff40b2642"

CCM
encrypt and tag NIST VPT AES-128 #7 (P=6, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"80bead98a05d1bb173cd4fca463b8fa3":"e479990bf082":"8a14a6d255aa4032ebff37a3d7":"bb4e706e73d21df66f64173859d47e247527cd9832e20dccff8548ed5f554108":"89c9246238878427f36b1f6c633e4542f32b50ca8edb"

CCM encrypt and tag NIST VPT AES-128 #8 (P=7, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"dc8ec91184ba18eae31ac2d3b252673f":"2a5775986551c8":"0da4c988f521f5648259f2bec2":"6d5573c9279897d7d1602d8a95c04bb5ca3fad2dbe89a024b3651eb227e73bb5":"4f259f2a718faea852a7c4358dfa9f5467357638acac90"

CCM encrypt and tag NIST VPT AES-128 #9 (P=8, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"19f97ef5318b8005fc7133fa31dd1236":"6d972a673fbe1ca1":"01ce9814c6329dbee1d02b1321":"85853f120981f33cf1d50fde6b8bc865fe988a9f12579acdb336f9f992b08b89":"2f12a7e7acecae5d2563309efc19368cdee8266538ca89d3"

CCM
encrypt and tag NIST VPT AES-128 #10 (P=9, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"c17944bfaeeb808eed66ae7242ab545f":"7caae2640e734539d3":"910b3db64df3728ca98219e01b":"edf64f98b3ab593cbcf68ab37a8c9472e49cb849d4a744deae925a5a43faf262":"0dae8b3ccf0b439f6ff8ee4a233dfb7753f6bfe321b3e26959"

CCM encrypt and tag NIST VPT AES-128 #11 (P=10, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"0fb9df6f638847f5de371f003dd938f4":"e10cc36bc1c5d3c646ab":"c9ddf61c052f3502ad6b229819":"4f9938d5bc3dcbe47f6b256d5e99723d0891e50c6175aba41b011e4686113c49":"7f797367de50be6dc04e4cf0d8c24189affd35060cb7ca3dd136"

CCM encrypt and tag NIST VPT AES-128 #12 (P=11, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"006ff7d3153caf906ec7929f5aef9276":"31be1b241

cae79c54c2446":"57db1541a185bd9cdc34d62025":"7d9681cac38e778fba11f4464f69ed9ebfea31b7ffcaf2925b3381c65d975974":"9dd8a4244fbdb30b624578a625c43233476bbb959acd9edebe2883"

CCM
encrypt and tag NIST VPT AES-128 #13 (P=12, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"026331e98aba9e8c23a9e8a91d0b0c97":"a82200ef3a08c390dec5cbf9":"bccfe69bba168b81cbdf7d018a":"26e011143a686a7224ddb8c5b1e5d31713fa22c386785e2c34f498ae56d07ed5":"adf4fc6f9be113066c09248fcb56a9c1a1c3bb16fbb9fbaedacdb12b"

CCM encrypt and tag NIST VPT AES-128 #14 (P=13, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"d32088d50df9aba14d9022c870a0cb85":"4b10788c1a03bca656f04f1f98":"e16c69861efc206e85aab1255e":"0eff7d7bcceb873c3203a8df74f4e91b04bd607ec11202f96cfeb99f5bcdb7aa":"89f15b1cb665a8851da03b874ca6f73242f2f227350c0277e4e72cdaa6"

CCM encrypt and tag NIST VPT AES-128 #15 (P=14, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"7301c907b9d2aaac355c5416ff25c59b":"484300aa3a506afcd313b49ead8d":"7304b65b6dab466273862c88b9":"2c5d114eff62c527cc2e03c33c595a80fe609bfc0fe13ce3380efe05d85cceac":"928ca58b0d373dc50c52afac787ce8eeb5d5b493661259a9d91ea31a5f7e"

CCM
encrypt and tag NIST VPT AES-128 #16 (P=15, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"38be46d271bf868c198052391f8a2147":"61bd1385be92097e866550a55278f0":"6758f67db9bfea5f0e0972e08b":"c6de3be97f11d0e2ab85c9353b783f25b37366a78a2012cecf5b7a87138b3c86":"7c9fa8d99b38f825315ece6a2613f55e902f296dcce870263ae50cda4fadae"

CCM encrypt and tag NIST VPT AES-128 #17 (P=16, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"70010ed90e6186ecad41f0d3c7c42ff8":"be322f58efa7f8c68a635e0b9cce77f2":"a5f4f4986e98472965f5abcc4b":"3fec0e5cc24d67139437cbc8112414fc8daccd1a94b49a4c76e2d39303547317":"8e4425ae573974f0f0693a188b525812eef08e3fb15f4227e0d989a4d587a8cf"

CCM encrypt and tag NIST VPT AES-128
#18 (P=17, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"79eae5baddc5887bdf3031fd1d65085b":"001343e6191f5f1738e7d19d4eec2b9592":"9da59614535d1fad35f2ece00f":"46603500af9e4e7a2f9545411a58b21a6efd21f2b5f315d02d964c09270145b3":"2162e27bfbf1d00f2404754a254665fd9270f0edb415993588b2535e2e0e4fd086"

CCM encrypt and tag NIST VPT AES-128 #19 (P=18, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"c14eda0f958465246fe6ab541e5dfd75":"617868ae91f705c6b583b5fd7e1e4086a1bb":"32b63ca7e269223f80a56baaaa":"733f8e7670de3446016916510dfe722ce671570121d91331a64feb3d03f210e6":"b2dc1e548b3d3f225a34082f4391980a0788b4cc36852fd64a423fb8e872252b248e"

CCM encrypt and tag NIST VPT AES-128 #20 (P=19, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"c5e7147f56ba4530b8799abab eb82772":"2f3bf0b5
66440912a1e47a0c07f1cfd39cb440":"bdd38e173fb20b981659c597d6":"3a069a2bfda44abbb0a82a97e5e9047258c8
03da2c66190d77149e0f010b3af9":"bd6265dcba9e14c59e515e395dc60bd053345fa6d7568c738e3a7fdf142d8f2d156
2c0"

CCM
encrypt and tag NIST VPT AES-128 #21 (P=20, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"78c46e3249ca28e1ef0531d80fd37c12":"4802422c
9b3b4459ba26e7863ad87b0c172cfe4b":"5de41a86ce3f3fb1b685b3ca4d":"e98a77f2a941b36232589486b05f427827
5588665a06d98aec98915cc5607e06":"daea2234ea433533bf0716abe1aa3844b6d3c51e9d5ca3d8ec5065630d2de071
7cdeb7d5"

CCM encrypt and tag NIST VPT AES-128 #22 (P=21, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"8883002bf13b3a94b2467225970df938":"d516bbff
452e7706c91c7ace3e9baa76d65ff7050f":"818a702d5c8ee973b34e9acda1":"545aeac737c0ca2a3d5e1fd966840c3a0
d71e0301abbe99c7af18d24cc7e9633":"b85242fdc06344f2bd9a97b408902ebcd22aece3d42f2da4dd4d817c9fa2d44b
c02163a0a9"

CCM encrypt and tag NIST VPT AES-128 #23 (P=22, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"5cea00ee44cfb9cfbb598d3812e380ef":"33bfd0713
f30fcac8f7f95920ac6d9b803ddd5480dd8":"948788a9c8188cb988430a7ebd":"50422c5e6a0fb8231b3bb6e2f896070
19be6ad92a4dae8e0fe3f9e486476004b":"b168747dea3ae0fbede4402af9a3dc3185d6d162f859d828101682de329237
88c70262b84814"

CCM
encrypt and tag NIST VPT AES-128 #24 (P=23, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"cb83f77751e72711401cbbf4f61aa0ed":"eede01b08
f9a303cdf14c99d7a45732972c6eff2a1db06":"c0b461b2e15b8b116ef9281704":"2bd112231f903fa0dff085db48a2e2
a96ec0199249b005d5ab4c2eab753f9ad0":"feb114b7bd3b43497b62454a675a632c3546d2802462c6af57647efda119
c59862cd5dd3904efc"

CCM encrypt and tag NIST VPT AES-128 #25 (P=24, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"43c1142877d9f450e12d7b6db47a85ba":"b506a6ba
900c1147c806775324b36eb376aa01d4c3eef6f5":"76becd9d27ca8a026215f32712":"6a59aacadd416e465264c15e1a
1e9bfa084687492710f9bda832e2571e468224":"14b14fe5b317411392861638ec383ae40ba95fefe34255dc2ec06788
7114bc370281de6f00836ce4"

CCM
encrypt and tag NIST VPT AES-192 #1 (P=0, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"086e2967cde99e90faaea8a94e168bf0e066c503a84

9a9f3":"":"929542cd690f1babcf1696cb03":"58f70bab24e0a6137e5cd3eb18656f2b5ccddc3f538a0000c65190e4a3668e71":"3bf9d93af6ffac9ac84cd3202d4e0cc8"

CCM encrypt and tag NIST VPT AES-192 #2 (P=1, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"992d38768b11a236945bd4b327c3728fac24c091238b6553":"1c":"b248a90b84b0122a5ad8e12760":"27cabc40da0e1eda0ea5f8abbb7c179e30776250a7b30d711b0e106c5ee9d84a":"1a96f58c3f38c44d1a345f3e2da6679f20"

CCM encrypt and tag NIST VPT AES-192 #3 (P=2, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"5012db40ff6ae23c1e1ce43768c5936c4400b0e79ae77f30":"0c6c":"b67e500b35d60ad7264240027c":"40affd355416200191ba64edec8d7d27ead235a7b2e01a12662273deb36379b8":"c996ef3d6ef9f981557506ecc8797bbaaaa7"

CCM
encrypt and tag NIST VPT AES-192 #4 (P=3, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"fa15cc7f0de294d7341b1fd79326c8be78e67822343c1992":"bcb898":"e5257aed2bda0495aa44591db4":"31a0338c3839931fa1dd5131cb796c4c6cfde9fb336d8a80ac35dec463be7a94":"68f08298d9a2147776dca9c1a42382bce323b2"

CCM encrypt and tag NIST VPT AES-192 #5 (P=4, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"b5330a8447d74a7987fb718cfae246b5c7e057991064eeaf":"b46b343e":"2ef29d62b40d8643848797cde8":"1225b036e6044df52314016760e92750de0936120395de750a2c54a7fa0cea82":"c2c39d6f9344e2de064f269d065a2a6108605916"

CCM encrypt and tag NIST VPT AES-192 #6 (P=5, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"30419145ae966591b408c29e5fd14d9112542909be5363f7":"8ceaeb89fd":"27e6b2a482bbc6f13702005708":"e04e81e860daf9696098c723085d8023c240ebe7a643131e35359ab04bd650fe":"ec9d5ed36243ddf77b33d8cf2963ba76fd4e19f3c5"

CCM
encrypt and tag NIST VPT AES-192 #7 (P=6, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"748ad503388a34041a7bdae6361d57894357c333bacf02ca":"24d6880aed7e":"518b79d194579b19f2d8845b70":"691dd98f61fd213b0840ec5a6f06ef9a1420be0d59bde5e43546347a2a865a94":"270120f9634ec15536e21d961c675070ec4cff9037bc"

CCM encrypt and tag NIST VPT AES-192 #8 (P=7, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"b930cca30a3fd230c237c8f3cc6792d0c4084dff5c18d775":"2a755e362373ef":"7574802fd82fe96c05431acd40":"1cf83928b6a9e525fe578c5c0f40c322be71b3092239bff954dd6883738d6d71":"f06238b0450fd1f4b6cab1383adb420c4724aa7bdfefb7"

CCM encrypt and tag NIST VPT AES-192 #9 (P=8, N=13, A=32, T=16)

depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"314c136999e41d137bd7ba17201a9fa406025868334e39b3":"4d54d8b06b204445":"65f7a0f4c0f5bba9d26f7e0ddb":"5c7ce4819b30b975ae6ce58dcc1bfa29a8b6dda8f4b76c7e23516487745e829c":"2baf90c490b11f9607482362ab3f157c42d0e9c6c5cffcf0"

CCM
encrypt and tag NIST VPT AES-192 #10 (P=9, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"a19f6be062ec0aaf33046bd52734f3336c85d8368bef86ab":"13511ae5ff6c6860a1":"7f2d07f8169c5672b4df7f6cac":"d68d5f763db6111c5d6324d694cb0236beab877daae8115ecb75d60530777b58":"b3859b757802ebd048467fd8e139eb9ee8fcdca45ed87dc1c8"

CCM encrypt and tag NIST VPT AES-192 #11 (P=10, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"de1c8263345081d2dfa9afdf37675971135e178df554a4d8":"f777aba1fa70f94e6de9":"a301bb82f91a582db01355c388":"9ad52c041390d0d4aaf65a4667c3239c95e7eae6178acc23fb4e70a852d483c6":"9d8bff6d2dcde77104ac6aba025abc01416a7ca9f096ab2529cb"

CCM encrypt and tag NIST VPT AES-192 #12 (P=11, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"248d36bd15f58e47fcf1c948272355821f8492e6e69f3661":"33709d9c7906e2f82dd9e2":"9e8d492c304cf6ad59102bca0e":"9ec08c7ed6b70823d819e9ab019e9929249f966fdb2069311a0ddc680ac468f5":"9114d36b79b1918b2720f40cddce66df9b4802f737bea4bd8f5378"

CCM
encrypt and tag NIST VPT AES-192 #13 (P=12, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"77a67fb504b961028633321111aac2c30eb6d71a8cf72056":"10554c062d269ff6dcd98493":"acadc0330194906f8c75ac287f":"8c18486d52571f70f2ba6a747aaa3d4b3ebc2e481ee1b70907dddb94bdfa0ca6":"7f8b0cad79b545e5addf0b04ff4b0f2b2a5067283210aba8630d0306"

CCM encrypt and tag NIST VPT AES-192 #14 (P=13, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"0d423519e4110c06063061323f8c7c95387776b6ee4e4b6e":"4021ff104ff1dbd91e46db249f":"39abe53826d9b8e300fe747533":"cdd9bf1b4f865e922c678ec4947ea0cb02e78bd5c1538f33aeb818ad3f47e519":"7953d3cd66d093785d123f65ba37f16761dd6aedbfc789ad96edf1490d"

CCM
encrypt and tag NIST VPT AES-192 #15 (P=14, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"a60cf7ceb62bf3118532bc61daa25ce946991047f951b536":"d64f9426febce6a84c954dd5ded5":"7499494faa44a7576f9ed5580d":"baa482c64eefd09118549a8968f44cfea7a436913a428e30aa4ab44802a4ba35":"f7580f17266d68237747bf57c7ed8242ac1a1979c5a9e7bc67d7698c7efa"

CCM encrypt and tag NIST VPT AES-192 #16 (P=15, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"82d4bc9aac298b09112073277205e1bf42176d1e6339b76c":"25a53fd3e476dc0860eeeea25fcb0c":"70325ef19e581b743095cd5eb1":"6d14bb2635c5d0ae83687f182427

9cf141173527e1b32d1baf8a27f7fe34a542":"4a1cfd0023557a184b929965b0a445cb3993ca35acf354cb2b4254ff672e7f"

CCM encrypt and tag NIST VPT AES-192 #17 (P=16, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"6873f1c6c30975aff6f08470264321130a6e5984ade324e9":"5051a0b0b6766cd6ea29a672769d40fe":"7c4d2f7cec04361f187f0726d5":"77743b5d83a00d2c8d5f7e10781531b496e09f3bc9295d7ae9799e64668ef8c5":"0ce5ac8d6b256fb7580bf6acc76426af40bce58fd4cd6548df90a0337c842004"

CCM
encrypt and tag NIST VPT AES-192 #18 (P=17, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"3cf8da27d5be1af024158985f725fd7a6242cbe0041f2c17":"f6dd2c64bf597e63263ccae1c54e0805fe":"07f77f114d7264a122a7e9db4f":"30457e99616f0247f1339b101974ea231904d0ef7bd0d5ee9b57c6c16761a282":"ce3031c3a70600e9340b2ddfe56aa72cffdc5e53e68c51ee55b276eb3f85d2cf63"

CCM encrypt and tag NIST VPT AES-192 #19 (P=18, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"b46a3a24c66eb846ca6413c001153dc6998970c12e7acd5a":"56d18d3e2e496440d0a5c9e1bcb464faf5bc":"b79c33c96a0a90030694163e2a":"ea9405d6a46cac9783a7b48ac2e25cc9a3a519c4658b2a8770a37240d41587fb":"01baba2e0d5b49d600d03a7ed84ee878926c0ca478f40a6fbde01f584d938a1c91bf"

CCM encrypt
and tag NIST VPT AES-192 #20 (P=19, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"7b71045ccef735bd0c5bea3cf3b7e16e58d9c62061a204e0":"890d05420d57e3b3d8dbef117fe60c3fa6a095":"2b9ecfd179242c295fe6c6fa55":"b89166f97deb9cc7fdeb63639eeafb145895b307749ec1a293b27115f3aa8232":"f842ff6662684de8785af275fa2d82d587de0687ebe35e883cbd53b82f2a4624c03894"

CCM encrypt and tag NIST VPT AES-192 #21 (P=20, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"dc7c67715f2709e150cceff020aaacf88a1e7568191acbcf":"f383bd3e6270876b74abbb5d35e7d4f11d83412c":"da56ea046990c70fa216e5e6c4":"f799818d91be7bab555a2e39f1f45810a94d07179f94fe1151d95ab963c47611":"377b5df263c5c74f63603692cbb61ea37b6d686c743f71e15490ca41d245768988719ede"

CCM encrypt and tag NIST VPT AES-192 #22 (P=21, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"f41e369a1599627e76983e9a4fc2e963dab4960b09ebe390":"81ad3f386bedcbf656ff535c63580d1f87e3c72326":"68ef8285b90f28bcd3cb1bacea":"dbe3e82e49624d968f5463ceb8af189fb3ad8b3b4122142b110d848a286dae71":"9f6028153e06d14d30b862a99a35413413c04a49dc6f68a03a11cf00d58f062a7b36465d13"

CCM

encrypt and tag NIST VPT AES-192 #23 (P=22, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"3289e59e3a7b29bf4a309afc253030bba4b9bdd64f0722f9":"53911a67b65738f87fc7c20d6db8044bde1af95838d1":"30259ce106e9bd7a8bacbaf212":"2870bd9a26c510e9a256920899bbc77a4eb9b53f927045a943d5ed6b13638cf3":"70cf37d4b6f7e707376b1574ce17c040b5143da47abb2fe9afafc2fccd98ccf63b0fdec30eac"

CCM encrypt and tag NIST VPT AES-192 #24 (P=23, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"40f1aff2e44d05f12126097a0f07ac0359ba1a609356a4e6":"8d98c580fb366f330dbfda20f91d99a0878b47efd14c6d":"0df3fc6396f851785fca9aa5ff":"e9699b20b0574fce8b5cbc4ef792eb96e2c1cce36b1b1f06ea2a95fe300633cc":"579cdf9da62a2df471e03450516adb4ce99ae0f70b1776a39c3b429a1f922fac0b59e29a122e43"

CCM
encrypt and tag NIST VPT AES-192 #25 (P=24, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"91f9d636a071c3aad1743137e0644a73de9e47bd76acd919":"4eaf9384cad976f65f98042d561d760b5a787330dc658f6c":"1bf491ac320d660eb2dd45c6c3":"3bdfd7f18d2b6d0804d779f0679aaa2d7d32978c2df8015ae4b758d337be81dd":"635530cab14e3d0a135bb6eebb5829412676e6dd4995f99cb7e17f235bd660e7e17b2c65320e9fd4"

CCM encrypt and tag NIST VPT AES-256 #1 (P=0, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"c6c14c655e52c8a4c7e8d54e974d698e1f21ee3ba717a0adfa6136d02668c476":"":"291e91b19de518cd7806de44f6":"b4f8326944a45d95f91887c2a6ac36b60eea5edef84c1c358146a666b6878335":"ca482c674b599046cc7d7ee0d00eec1e"

CCM encrypt and tag NIST VPT AES-256 #2 (P=1, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"cc49d4a397887cb57bc92c8a8c26a7aac205c653ef4011c1f48390ad35f5df14":"1a":"6df8c5c28d1728975a0b766cd7":"080f82469505118842e5fa70df5323de175a37609904ee5e76288f94ca84b3c5":"a5f24e87a11a95374d4c190945bf08ef2f"

CCM
encrypt and tag NIST VPT AES-256 #3 (P=2, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"36b0175379e7ae19c277fe656a2252a82796309be0f0d4e1c07fdde88aca4510":"be80":"021bd8b551947be4c18cf1a455":"b5c6e8313b9c68e6bb84bffd65fa4108d243f580eab99bb80563ed1050c8266b":"ecacc3152e43d9efea26e16c1d1793e2a8c4"

CCM encrypt and tag NIST VPT AES-256 #4 (P=3, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"ddb739acda6c56ec9aefc4f4cbc258587f443da4e76ddfa85dbe0813a8784944":"db457c":"0bddf342121b82f906368b0d7b":"887486fff7922768186363ef17eb78e5cf2fab8f47a4eb327de8b16d63b02acb":"54473c3f65d6be431e79700378049ac06f2599"

CCM encrypt and tag NIST VPT AES-256 #5 (P=4, N=13, A=32, T=16)

depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"62b82637e567ad27c3066d533ed76e314522ac5c53851a8c958ce6c64b82ffd0":"87294078":"5bc2896d8b81999546f88232ab":"fffb40b0d18cb23018aac109bf62d849adca42629d8a9ad1299b83fe274f9a63":"2bc22735ab21dfdcfe95bd83592fb6b4168d9a23"

CCM
encrypt and tag NIST VPT AES-256 #6 (P=5, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"bc29a16e19cfbe32bf4948e8e4484159bc819b7eec504e4441a1a98ca210e576":"3e8c6d1b12":"4f18bcc8ee0bbb80de30a9e086":"574931ae4b24bdf7e9217eca6ce2a07287999e529f6e106e3721c42dacf00f5d":"45f3795fcf9c66e1a43103d9a18f5fba5fab83f994"

CCM encrypt and tag NIST VPT AES-256 #7 (P=6, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"5f4b4f97b6aa48adb3336c451aac377fde4adf47897fd9ccdf139f33be76b18c":"1b62ad19dcac":"7a76eac44486afdb112fc4aab9":"a66c980f6621e03ff93b55d5a148615c4ad36d6cbdd0b22b173b4b1479fb8ff7":"4ad1fcf57c12b14e0e659a6305b4aeffae82f8a66c94"

CCM encrypt and tag NIST VPT AES-256 #8 (P=7, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"f7aaeff3a1dc0cc5ecf220c67ad9f6dda060b4f1be3cc609cb4f18b2342a88a2":"d48daa2919348d":"d0d6871b9adc8623ac63faf00f":"e97175c23c5b47da8ce67811c6d60a7499b3b7e1347ad860519285b67201fe38":"eb32ab153a8e092fa325bafc176a07c31e6cc0a852d288"

CCM
encrypt and tag NIST VPT AES-256 #9 (P=8, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"493e14623cd250058a7fc66a3fee0c24b6e363b966c2314aff53b276b6c2ea7b":"e5653e512d8b0b70":"fe2d8ae8da94a6df563f89ce00":"579a637e37a0974cd2fc3b735d9ed088e8e488ffe210f043e0f9d2079a015ad6":"75d31f8d47bee5c4e2ba537355ae8ab25cc9ed3511ff5053"

CCM encrypt and tag NIST VPT AES-256 #10 (P=9, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"b23255372455c69244a0210e6a9e13b155a5ec9d6d0900e54a8f4d9f7a255e3a":"615d724ae94a5daf8d":"274846196d78f0af2df5860231":"69adcae8a1e9a3f2fe9e62591f7b4c5b19d3b50e769521f67e7ea8d7b58d9fc8":"f019ae51063239287d896e7127f17d13f98013b420219eb877"

CCM
encrypt and tag NIST VPT AES-256 #11 (P=10, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"dbf06366f766e2811ecd5d4384d6d08336adc37e0824d620cf0d9e7fd1e7afa9":"2e3cf0af8c96c7b22719":"b3503ed4e277ed9769b20c10c0":"9ae5a04baa9d02c8854e609899c6240851cbc83f81f752bc04c71affa4eed385":"e317df43ab46eb31be7e76f2730d771d56099a0c8d2703d7a24e"

CCM encrypt and tag NIST VPT AES-256 #12 (P=11, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"4dd555bd3a5253a90b68b5d4d46bd050340ee07ddad3a72048c657b5d76bb207":"8015c0f07a7acd4b1cbdd2":"bdb1b82ba864893c2ee8f7426c":"9bcc5848e928ba0068

f7a867e79e83a6f93593354a8bfcfc306aeeb9821c1da1":"8e9f80c726980b3d42e43a6512a0481255b729a10f9edb5f07c60c"

CCM encrypt and tag NIST VPT AES-256 #13 (P=12, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"d3ad8cda9a0d91a205c4c05665728bb255d50a83403c9ab9243fcbbe95ae7906":"a203aeb635e195bc33fd42fa":"0b5f69697eb1af24e8e6fcb605":"ea26ea68facdac3c75ba0cdf7b1ad703c9474af83b3fbfc58e548d776b2529b9":"62666297a809c982b50722bd56bc555899345e0404b2938edf33168e"

CCM
encrypt and tag NIST VPT AES-256 #14 (P=13, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"e300fc7a5b96806382c35af5b2c2e8e26382751b59010d4b1cfc90a4a9cb06df":"8714eb9ecf8bdb13e919de40f9":"55b59eb434dd1ba3723ee0dc72":"9b1d85384cb6f47c0b13514a303d4e1d95af4c6442691f314a401135f07829ec":"ba6063824d314aa3cbab14b8c54c6520dac0f073856d9b9010b7857736"

CCM encrypt and tag NIST VPT AES-256 #15 (P=14, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"3ae5be5904bae62609ac525e2d1cad90133447573d7b608975a6a2b16cb2efc0":"959403e0771c21a416bd03f38983":"61bf06b9fa5a450d094f3ddcb5":"0245484bcd987787fe97fda6c8ffb6e7058d7b8f7064f27514afaac4048767fd":"37a346bc4909965c5497838251826385a52c68914e9d1f63fd297ee6e7ed"

CCM
encrypt and tag NIST VPT AES-256 #16 (P=15, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"fab62b3e5deda7a9c1128663cc81c44b74ab1bfe70bc1c9dec7c7fd08173b80a":"54be71705e453177b53c92bbf2ab13":"a5c1b146c82c34b2e6ebeceb58":"5e60b02b26e2d5f752eb55ea5f50bb354a6f01b800cea5c815ff0030b8c7d475":"788db949697b8cd9abbc74ed9aa40cd6852dc829469368491149d6bb140071"

CCM encrypt and tag NIST VPT AES-256 #17 (P=16, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"ee8ce187169779d13e443d6428e38b38b55dfb90f0228a8a4e62f8f535806e62":"d15f98f2c6d670f55c78a06648332bc9":"121642c4218b391c98e6269c8a":"718d13e47522ac4cdf3f828063980b6d452fcdcd6e1a1904bf87f548a5fd5a05":"cc17bf8794c843457d899391898ed22a6f9d28fcb64234e1cd793c4144f1da50"

CCM encrypt and tag NIST VPT AES-256 #18 (P=17, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"7da6ef35ad594a09cb74daf27e50a6b30d6b4160cf0de41ee32bbf2a208b911d":"b0053d1f490809794250d856062d0aaa92":"98a32d7fe606583e2906420297":"217d130408a738e6a833931e69f8696960c817407301560bbe5fbd92361488b4":"a6341ee3d60eb34a8a8bc2806d50dd57a3f628ee49a8c2005c7d07d354bf80994d"

CCM

encrypt and tag NIST VPT AES-256 #19 (P=18, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"0786706f680c27b792d054faa63f499a8e6b5ddb90502946235bf74c022d772c":"6a26677836d65bd0d35a027d278b2534e7df":"f61ef1c8c10a863efeb4a1de86":"67874c808600a27fcab34d6f69cc5c730831ad4589075dd82479823cb9b41dc3":"d1c1f3c60603359c7d6a707f05ecb2296f8e52f2210b7a798ad5c778ee7cfd7fe6e0"

CCM encrypt and tag NIST VPT AES-256 #20 (P=19, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"bac55f9847d93325bf5071c220c0a3dfeb38f214292d47b4acb7b0a597fe056f":"c1a994dc198f5676ea85801cd27cc8f47267ec":"05b50c458adbba16c55fcc454d":"89ad6ae1e550975eaa916a62615e6b6a66366a17a7e06380a95ea5cdcc1d3302":"7c9b138177590edaafec4728c4663e77458ffbe3243faec177de4a2e4a293952073e43"

CCM
encrypt and tag NIST VPT AES-256 #21 (P=20, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"8beedeb85d42c2a7fa6f7237b05acb197dd8e1672471ac878064fe5319eab876":"7b125c3b9612a8b554913d0384f4795c90cd387c":"8479bdfad28ebe781e9c01a3f6":"7aebdfd955d6e8a19a701d387447a4bdd59a9382156ab0c0dcd37b89419d6eff":"6cc611d816b18c6847b348e46a4119465104254a04e2dfeeeac9c3255f6227704848d5b2"

CCM encrypt and tag NIST VPT AES-256 #22 (P=21, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"c3a0c126cad581012151c25cf85a44472c23f83b6095b6004f4f32cd60ec2db2":"73b09d18554471309141aa33b687f9248b50fe3154":"94ab51ce75db8b046d6ab92830":"2a243246bfe5b5ab05f51bf5f401af52d5bbaa2549cf57a18e197597fe15dd8c":"b7e8264ca70fd2a4fb76f20a8ad5da3c37f5893fb12abeeaef1187f815ca481ed8ddd3dd37"

CCM encrypt and tag NIST VPT AES-256 #23 (P=22, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"9cdebaeee8690b68751070691f49593668a6de12d3a948b38ddbd3f75218b2d4":"3cbb08f133270e4454bcaaa0f20f6d63c38b6572e766":"af1a97d43151f5ea9c48ad36a3":"f5353fb6bfc8f09d556158132d6cbb97d9045eacdc71f782bcef62d258b1950a":"3966930a2ae8fdd8f40e7007f3fde0bd6eb48a46e6d26eef83da9f6384b1a2bda10790dadb3f"

CCM
encrypt and tag NIST VPT AES-256 #24 (P=23, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"d34264a12c35cdd67ac105e2826b071e46f8131d1e325f8e0ae80a6447375135":"79ac1a6a9eca5e07ce635bfd666ef72b16f3f2e140d56c":"3891e308b9f44c5b5a8b59004a":"0cda000ed754456a844c9ed61843deea9dadf5e723ea1448057712996d660f8c":"1abcc9b1649deaa0bfa7dcd23508282d9c50ca7fee72486950608d7bcb39dcf03a2cab01587f61"

CCM encrypt and tag NIST VPT AES-256 #25 (P=24, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"4ad98dbef0fb2a188b6c49a859c920967214b998435a00b93d931b5acecaf976":"9cea3b061e5c402d48497ea4948d75b8af7746d4e570c848":"00d772b07788536b688ff2

b84a":"5f8b1400920891e8057639618183c9c847821c1aae79f2a90d75f114db21e975":"f28ec535c2d834963c85814ec4173c0b8983dff8dc4a2d4e0f73bfb28ad42aa8f75f549a93594dd4"

CCM
encrypt and tag NIST VNT AES-128 #1 (P=24, N=7, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"c0425ed20cd28fda67a2bcc0ab342a49":"4f065a23eeca6b18d118e1de4d7e5ca1a7c0e556d786d407":"37667f334dce90":"0b3e8d9785c74c8f41ea257d4d87495ffbbb335542b12e0d62bb177ec7a164d9":"768fccdf4898bca099e33c3d40565497dec22dd6e33dcf4384d71be8565c21a455db45816da8158c"

CCM encrypt and tag NIST VNT AES-128 #2 (P=24, N=8, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"0b6256bd328a4cda2510d527c0f73ed4":"78a292662b8e05abc2d44fbefd0840795e7493028015d9f2":"21fd9011d6d9484a":"66ff35c4f86ad7755b149e14e299034763023e7384f4af8c35277d2c7e1a7de2":"5a0be834c57b59d47a4590d8d19a1206d3c06e937a9b57f74034d9fdb43c3f48932aa72177b23bf6"

CCM
encrypt and tag NIST VNT AES-128 #3 (P=24, N=9, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"afdccc84f257cb768b7ad735edbd1990":"56d0942490e546798f30d3c60ad4e3e110fc04f5b1c1fa83":"b7776aa998f4d1189b":"9f9ac464de508b98e789243fdb32db458538f8a291ed93ddf8aeaacfbfc371aa":"96f124c74fd737819008ddef440320f4a3733d0062c83c893e259aecf12ba08f2a2e966a3341d6d4"

CCM encrypt and tag NIST VNT AES-128 #4 (P=24, N=10, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"6ccb68d3838d4ddf660b9cd904cad40f":"5ea35c082e2b190e9d98e6b2daad8672f587b4f2968072fc":"c4fb7519a19f13d9d1fc":"092e64fef08b5655a86cdb8de63ffaa7772e8730844e9016141af8bad2216246":"cda5fe3d15d00150b99120c7f206b88a4c2c4a39ca9143425603ab284a73a38cc916f8b653c92ab4"

CCM encrypt and tag NIST VNT AES-128 #5 (P=24, N=11, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"e6ab9e70a4fb51b01c2e262233e64c0d":"ba15916733550d7aa82b2f6b117cd3f54c83ddc16cd0288a":"74e689eb5af9441dd690a6":"42f6518ee0fbe42f28e13b4bb2eb60517b37c9744394d9143393a879c3e107c7":"dcc151443288f35d39ed8fae6f0ce1d1eb656f4f7fd65c0b16f322ce85d7c54e71ac560fd4da9651"

CCM
encrypt and tag NIST VNT AES-128 #6 (P=24, N=12, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"005e8f4d8e0cbf4e1ceeb5d87a275848":"b6f345204526439daf84998f380dcfb4b4167c959c04ff65":"0ec3ac452b547b9062aac8fa":"2f1821aa57e5278ffd33c17d46615b77363149dbc98470413f6543a6b749f2ca":"9575e16f35da3c88a19c26a7b762044f4d7bbbafeff05d754829e2a7752fa3a14890972884b511d8"

CCM encrypt and tag NIST VNT AES-128 #7 (P=24, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"ac87fef3b76e725d66d905625a387e82":"959403e0771c21a416bd03f3898390e90d0a0899f69f9552":"61bf06b9fa5a450d094f3ddcb5":"0245484bcd987787fe97fda6c8ffb6e7058d7b8f7064f27514afaac4048767fd":"cabf8aa613d5357aa3e70173d43f1f202b628a61d18e8b572eb66bb8213a515aa61e5f0945cd57f4"

CCM
encrypt and tag NIST VNT AES-192 #1 (P=24, N=7, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"ceb009aea4454451feadf0e6b36f45555dd04723baa448e8":"c8d275f919e17d7fe69c2a1f58939dfe4d403791b5df1310":"764043c49460b7":"6e80dd7f1badf3a1c9ab25c75f10bde78c23fa0eb8f9aaa53adefbf4cbf78fe4":"8a0f3d8229e48e7487fd95a28ad392c80b3681d4fbc7bbfd2dd6ef1c45d4ccb723dc074414db506d"

CCM encrypt and tag NIST VNT AES-192 #2 (P=24, N=8, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"1dd56442fa09a42890b1b4274b950770ea8beea2e048193d":"bd92d6744cde446fc8621625658fc4bc00dcb97f06195ad7":"ad749d596d88a4b4":"c67219909828adef64422286008e1e306867a1c0b3da95444507a68b45c953e4":"076cffd0ca978fe2bad411ced45a090abafb22a99896f6a75a1969276aa2b0cdb37ccaf2845dbf6e"

CCM encrypt and tag NIST VNT AES-192 #3 (P=24, N=9, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"8cc622645065c72d0d2aca75802cf1bbbd81096721627c08":"597b3614ff9cd567afd1aad4e5f52cc3fa4ca32b9b213c55":"cd84acbe9abb6a990a":"447b6f36acdad2d1cfd6e9a92f4055ad90142e61f4a19927caea9dbe634d3208":"2d7fb83e6621eed9073e0386d032c6941bef37b2cf36a4c6c5e36222d17c6fb0631c3f560a3ce4a4"

CCM
encrypt and tag NIST VNT AES-192 #4 (P=24, N=10, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"ab72eef2aba30205c986e2052d6e2c67881d24ae5fceaa8f":"2a794b84fc9e4a7e6d70a82b5141fd132177a86b4e8fc13a":"d7a46e726ed43f1580eb":"baa86f14271b2be7dbb37ddc7c95ce4857e57aa94624d594d7bd6ceeaada8d5f":"2d7f76464417613bb61d3657481346b74fc9d6abc6a3babd39365dce86859cd82395d11bfc8cf188"

CCM encrypt and tag NIST VNT AES-192 #5 (P=24, N=11, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"af84c6f302c59aeee6d5728ed5da2e3c64a5a781c52c4d1b":"6db41aeb5f7c24df8929dbc30483b3c7934b3bd1cdce5bb9":"df990c42a268950677c433":"a6ab5d78427f297a4b7e21f1091ff3a5b20caa3fe1cbcb09459d9df596a6c8e1":"8c9328258bf71970d33e23a3ff81cc1c9cbe196a1294264bfd6a7255e4801963bb30a63de3fc5b82"

CCM
encrypt and tag NIST VNT AES-192 #6 (P=24, N=12, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"d49b255aed8be1c02eb6d8ae2bac6dcd7901f1f61df

3bbf5":"062eafb0cd09d26e65108c0f56fcc7a305f31c34e0f3a24c":"1af29e721c98e81fb6286370":"64f8a0eee5487a4958a489ed35f1327e2096542c1bdb2134fb942ca91804c274":"721344e2fd05d2ee50713531052d75e4071103ab0436f65f0af2a663da51bac626c9f4128ba5ec0b"

CCM encrypt and tag NIST VNT AES-192 #7 (P=24, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"36ad1e3fb630d1b1fbccfd685f44edd8984427b78deae7a9":"8b9db1c8f9b4892a5654c85467bcffa2e15e28392c938952":"3af625df8be9d7685a842f260e":"308443033ecd4a814475672b814b7c6d813d0ec2a0caeecbcaba18a2840cdb6c":"6bc6890fee299c712fb8d9df9c141f24ee1572b8f15112c2f8c99ccf2d82788cf613a61d60dae458"

CCM encrypt and tag NIST VNT AES-256 #1 (P=24, N=7, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"553521a765ab0c3fd203654e9916330e189bdf951feee9b44b10da208fee7acf":"644eb34b9a126e437b5e015eea141ca1a88020f2d5d6cc2c":"aaa23f101647d8":"a355d4c611812e5f9258d7188b3df8851477094ffc2af2cf0c8670db903fbbe0":"27ed90668174ebf8241a3c74b35e1246b6617e4123578f153bdb67062a13ef4e986f5bb3d0bb4307"

CCM
encrypt and tag NIST VNT AES-256 #2 (P=24, N=8, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"472bf7946bce1d3c6f168f4475e5bb3a67d5df2fa01e64bce8bb6e43a6c8b177":"59eb45bbbeb054b0b97334d53580ce03f699ac2a7e490143":"790134a8db83f2da":"a7a86a4407b7ecebc89434baa65ef173e88bd2dad9899b717ca578867c2d916f":"db4961070f528ccd1a5a0681ee4d0ce3515fb890bccedc2dbc00b1d8b2bc393a8d09e87af7811f55"

CCM encrypt and tag NIST VNT AES-256 #3 (P=24, N=9, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"58ae7965a508e8dd2eda69b5d888a28a1cb3783bad55d59d5b0da87137b72e93":"e61bad17640ecff926d0b0238271ee4c9f8e801dd7243e9e":"caa3d928d2bf2b7f2c":"304678b3ffd3200e33a8912bcb556b3cfec53ca17f70ecba00d359f9f51d3e3b":"7bb1137c14cb4d324a4a8f1115c619ebf74927f0bed60a8d5a9140ff50dc4da375c7d2de80de097f"

CCM
encrypt and tag NIST VNT AES-256 #4 (P=24, N=10, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"aecc5e18088bf9fd7b17f089bdd5607b69903b04b726361f8a81e221b1c91891":"d4291c99901345afe29f58912a414a7498f37b44362bdf3c":"c527d309ab29ee91c5fc":"8f9a73e7bc1c11e2919020ba3a404cbddf861e9e78477218e3be2cd4337b278d":"392784a9e0b14bcd37639ec5409d6ead3e75f855e5a92c33ffc040ef3977e0035ce6ea6d157c18d3"

CCM encrypt and tag NIST VNT AES-256 #5 (P=24, N=11, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"97bc7482a87ba005475dfa3448f59d4b3f9c4c969d08b39b1b21ef965c0f5125":"b99bf4dc781795fc4d3a8467b06e1665d4e543657f23129f":"0bcf78103ec52d6df28887":"049c10f0cb37ae08eae2d0766563b7c5a8454f841c2061a4f71a0a2158ae6ce5":"0d3891fa0caac1f7ebe41b480920ffd34d4155064c24f3b17a483163dd8f228d1f20cd4f86cf38fd"

CCM
encrypt and tag NIST VNT AES-256 #6 (P=24, N=12, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"d6ff67379a2ead2ca87aa4f29536258f9fb9fc2e91b0ed18e7b9f5df332dd1dc":"98626ffc6c44f13c964e7fcb7d16e988990d6d063d012d33":"2f1d0717a822e20c7cd28f0a":"d50741d34c8564d92f396b97be782923ff3c855ea9757bde419f632c83997630":"50e22db70ac2bab6d6af7059c90d00fbf0fb52eee5eb650e08aca7dec636170f481dcb9fefb85c05"

CCM encrypt and tag NIST VNT AES-256 #7 (P=24, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"4a75ff2f66dae2935403cce27e829ad8be98185c73f8bc61d3ce950a83007e11":"205f2a664a8512e18321a91c13ec13b9e6b633228c57cc1e":"46eb390b175e75da6193d7edb6":"282f05f734f249c0535ee396282218b7c4913c39b59ad2a03ffaf5b0e9b0f780":"58f1584f761983bef4d0060746b5d5ee610ecfda31101a7f5460e9b7856d60a5ad9803c0762f8176"

CCM encrypt and tag NIST VADT AES-128 #1 (P=24,
N=13, A=0, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"d24a3d3dde8c84830280cb87abad0bb3":"7c86135ed9c2a515aaae0e9a208133897269220f30870006":"f1100035bb24a8d26004e0e24b":"":"1faeb0ee2ca2cd52f0aa3966578344f24e69b742c4ab37ab1123301219c70599b7c373ad4b3ad67b"

CCM encrypt and tag NIST VADT AES-128 #2 (P=24, N=13, A=1, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"08b0da255d2083808a1b4d367090bacc":"1b156d7e2bf7c9a25ad91cff7b0b02161cb78ff9162286b0":"777828b13679a9e2ca89568233":"dd":"e8b80af4960d5417c15726406e345c5c46831192b03432eed16b6282283e16602331bcca9d51ce76"

CCM encrypt and tag NIST VADT AES-128 #3 (P=24, N=13, A=2, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"1538cc03b60880bf3e7d388e29f27739":"e7b819a853ffe79baaa72097ff0d04f02640ae62bcfd3da5":"9e734de325026b5d7128193973":"c93c":"1d8f42f9730424fa27240bd6277f4882604f440324b11b003ca01d874439b4e1f79a26d8c6dc433a"

CCM encrypt and
tag NIST VADT AES-128 #4 (P=24, N=13, A=3, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"f149e41d848f59276cfddd743bafa9a9":"9759e6f21f5a588010f57e6d6eae178d8b20ab59cda66f42":"14b756d66fc51134e203d1c6f9":"f5827e":"f634bf00f1f9f1f93f41049d7f3797b05e805f0b14850f4e78e2a23411147a6187da6818506232ee"

CCM encrypt and tag NIST VADT AES-128 #5 (P=24, N=13, A=4, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"9a57a22c7f26feff8ca6cceff214e4c2":"035c516776c706a7dd5f181fa6aa891b04dd423042ea0667":"88f30fd2b04fb8ddbce8fc26e6":"a95bdff6":"b92f7ec2ebecebdbd2977b3874e61bf496a382153b2529fc9b6443a35f329b2068916fb6ab8227eb"

CCM encrypt and tag NIST VADT AES-128 #6 (P=24, N=13, A=5, T=16)

depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"54caf96ef6d448734700aadab50faf7a":"c69f7c5a50f3e72123371bbfd6bdf532b99ef78500508dfe":"a3803e752ae849c910d8da36af":"5f476348dd":"20c43ad83610880249f1632dd418ec9a5ed333b50e996d1a4e5a32fbe7961b832b722bc07a18595b"

CCM
encrypt and tag NIST VADT AES-128 #7 (P=24, N=13, A=6, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"cc0c084d7de011e2f031616a302e7a31":"15b369889699b6de1fa3ee73e5fe19814e46f129074c965b":"f0b4522847f6f8336fe534a4e7":"da853a27aee2":"f39755d160a64611368a8eccf6fcbc45ef7f1f56240eb19a2e3ca4ec3c776ab58843f617d605fd72"

CCM encrypt and tag NIST VADT AES-128 #8 (P=24, N=13, A=7, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"d7572ed0e37261efa02f8c83e695efdc":"1edef80c57d17f969f8bde10ab38a1a8811a124de72c526e":"f4f96d7b4384a3930b3d830f82":"922340ec94861f":"de14558cc686e1836f1f121ea1b941a9ebd4f0fb916dc870fd541b988a801cb5751c7faaf5b0c164"

CCM encrypt and tag NIST VADT AES-128 #9 (P=24, N=13, A=8, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"98a42d7a0c5917deaf3b4de3f0cbe0a1":"9aa9c8358117564371366beeec923051ef433252197aaad5":"03d33ab0c2df7bfce88b5ee4c4":"2d5438b728b950d9":"9ff942baa60f440c17a78e9581216b9a947a67f04d54911feecfff971fdfaa856310b014aa59c978"

CCM
encrypt and tag NIST VADT AES-128 #10 (P=24, N=13, A=9, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"2a68e3fe746f593c1b97cb637079c3e5":"13b4a874888db0e5d8fd814b5e7e04f7fdfbc1601ccc02bc":"cd62d0f27b7f4864dc7c343acd":"abe4f1d3812bfe3ccf":"032835a3dbf688d09cf2a32a92b101959d33ff47500f92f4fd49840440f866d1a22b0854996111d8"

CCM encrypt and tag NIST VADT AES-128 #11 (P=24, N=13, A=10, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"46b067cf9b1a28cf187002e90b14e130":"cc0915194218d4536e467433cd6d79ff1d9eb9ff160ab684":"bad8c03292bf01cfd8d34f860c":"8d65880eddb9fd96d276":"bd56edc015692c6ab9bec493a9893863598414a3d11a6a0f27ecdcb257d0d30491e5bf1aa8f90958"

CCM encrypt and tag NIST VADT AES-128 #12 (P=24, N=13, A=11, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"e94dac9c90984790a7c0c867536615ff":"4d64461c55eb16bf7b9120f22be349598f2f394da8460dc6":"c19f06f91e645d4199365f18c0":"537038b5357e358a930bd6":"e9fc5004c2359724e1e4411ae6f834ef6bea046d549753c88790c1648f461a31c84e62ea8592a074"

CCM
encrypt and tag NIST VADT AES-128 #13 (P=24, N=13, A=12, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"f6bb5d59b0fa9de0828b115303bf94aa":"011fc50329bfd63a85ebd4f7693363602f1a4147371270b7":"05358f33e1fc6a53ab5a5c98ce":"040b25771239cc2a39446e3c":"4

432d7eb42980734d34f19c50cf8abf71ac1b19ed75a727854e5d050a405f755047d09cb0f49546a"

CCM encrypt and tag NIST VADT AES-128 #14 (P=24, N=13, A=13, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"d1da2e961e78063af8de41865b226873":"8e5fa1a6662a8378cda15697e926841594f2f394fa5a34ab":"03739f5474857006340cce554d":"e3afd091d2b588465872a6300f":"ca0d95e3ff186ad6b88d45fc4079e6b7b4a615e7e8dd5f4742d522cc9dc19c47a4fa0b1528069cf8"

CCM encrypt and tag NIST VADT AES-128 #15 (P=24, N=13, A=14, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"1eee667267ef10b03624cf9c341e3f75":"798e31cce0a83702a95171fb1162a17b9ce00ec3592ce262":"0630a3eae27e505c61c56e6560":"d24651ef0561282d3e20e834960c":"f3c3e52f1a1ff528a8d3783ee4e75f114e3e6416334815d2d9236d5c5c9319092078411b72c51ba8"

CCM
encrypt and tag NIST VADT AES-128 #16 (P=24, N=13, A=15, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"dbbd26f5d9e970e4e384b2273961be5a":"553714e17a208a2eceb847a4a2d95088388b1ac8d8ca43e0":"0b1eabe504ef4822542e397fec":"477937301c83ba02d50760b603e0ea":"1c80213268bad5402c4dc9b5d836ab7499810d0d8a974716df9a0e986ab2890736423bb3772cec3e"

CCM encrypt and tag NIST VADT AES-128 #17 (P=24, N=13, A=16, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"10a7720f2e18f739c26924925af6b670":"e59782a9aea45f467b90e51a0fdf166baba05663def2d8b6":"8c4e7813ab9bce9dafee01c628":"a209941fab710fda38d11c68b13d930f":"e357b1ccdaca6f3506dc45279c2e4c59f5307a5fd6a99cd72341ea8c0785569973f90ee9ee645acc"

CCM
encrypt and tag NIST VADT AES-128 #18 (P=24, N=13, A=17, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"6bffab1f4f4c1ff66b4a669b515b2f8d":"d91b12e8655dd92b1332fc1d71c391c96a17111562d90ba3":"ddb34d5e0140fb96d690e1a2b7":"5cbba9ea778e01af00afb2a934f28c7211":"d302e5b2d5d90433186b804cd7717e2db2f22cdc34fb2942ab30780a2c4f12af8f35350d65284c59"

CCM encrypt and tag NIST VADT AES-128 #19 (P=24, N=13, A=18, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"ae6136df9ab43631ef143515dacedbe7":"6a493c5ef3769ccc4101dbb2eb36e1e5bbc577a057ce0731":"c5c445792208a50c8e93d64aa3":"e04006b68c83a5dd4ceac3cde238e48895ae":"c7584c0203c2535c5702c6ae93b7cbfb066f4a055c627a180d6d676d11fce907b5c93fa1ed7bff2b"

CCM encrypt and tag NIST VADT AES-128 #20 (P=24, N=13, A=19, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"f1908328edf2996ebfc9655472ca5ad0":"eede01b08f9a303cdf14c99d7a45732972c6eff2a1db06eb":"4c693364546930b6c5250e2699":"4a3634e5028df97fbe00eb016e8ea4f1918faa":"90c850790b0b380f5aeb2488fdf43c9d5ef1759861e86f6e52570e769629dcc2e568737ba53a1195"

CCM

encrypt and tag NIST VADT AES-128 #21 (P=24, N=13, A=20, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"61cb8eb792e95d099a1455fb789d8d16":"6ad541695a37c32d73ff6d5f870abd5b0f362a8968c4fce0":"1f37b3e59137f2a60dc09d16ac":"09db3efac9473f713da630ae92c2c8604c61c51e":"e65fcc975865c1499b088b58ba163283085d8ca68dc3b235d89756e5d78753ef22c012ae34b39a20"

CCM encrypt and tag NIST VADT AES-128 #22 (P=24, N=13, A=21, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"be1ed49e2cb0caf6b6a0940c58453b93":"a9eec383f63892521e4616fcbadc5485942ffaf4669c43a7":"b78ad129457681fa7346435b97":"161d92c7df1ebb0924719e066e08b95eb4914a5eda":"949be340720c4fdc4adc05cb777dd81a2549628d33fba07e62d2b338a7b34ebd9d85c244c952d681"

CCM encrypt and tag NIST VADT AES-128
#23 (P=24, N=13, A=22, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"34ab6fd7f54a2e0276fcb7cf1e203aba":"8d164f598ea141082b1069776fccd87baf6a2563cbdbc9d1":"6091afb62c1a8eed4da5624dd7":"1ab5cc3d7b01dc74e6cf838bb565fea3187d33d552a2":"0d30ab07153b5153637969e6bd3539448c541e42b3d432fd7ef14622a9b621d1721b944c60f7fd67"

CCM encrypt and tag NIST VADT AES-128 #24 (P=24, N=13, A=23, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"ea96f90fbae12a857f5c97e0cba57943":"49db80f22bc267a70e5636dfbc8a21c83d9691fe4b9c3051":"21cc46d9ced1539b0ad946e600":"105258d2f25f62675aee975cfdb668aff833f05b61eb2a":"d2fcc8b7809b5fc07e44083e437d8180157f1782a9ce9f65c7fa9ee2e7cdc1b755258f2212a8a8f4"

CCM encrypt and tag NIST VADT AES-128 #25 (P=24, N=13, A=24, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"35b403a15212097085d6e2b77ec3d4f2":"7dd7396db6613eb80909a3b8c0029b624912aabedda0659b":"daa423bf9256c3fcc347a293aa":"d3c0ed74e5f25e4c1e479e1a51182bb018698ec267269149":"5b00cf8a66baa7fe22502ed6f4861af71fa64b550d643f95eee82c19ecba34280604b58d92dacd3f"

CCM
encrypt and tag NIST VADT AES-128 #26 (P=24, N=13, A=25, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"7a459aadb48f1a528edae71fcf698b84":"0b3d947de8632dc8ff752f619ba7c84716fac7a23e101641":"fa4616b715ea898772b0e89dd4":"0c0b4a45df5c3919c1e1669c5af5d398d9545e44307d95c481":"7db9f3f7dc26fc2adf58d4525d26d5601e977de5a7c33911a1138cff7b624f9908b5b4d7e90a824a"

CCM encrypt and tag NIST VADT AES-128 #27 (P=24, N=13, A=26, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"ca748225057f735f712ecc64791367f0":"e92cd0cb97afe4fb00c4f12e9b9abe1d08db98f49a27f461":"1341a6998eb1f50d4b710a13ac":"5fb96b045f494808c02014f06074bd45b8a8ad12b4cb448ec162":"82b666694232e86e82295beae66ae67d56aceb5d6b1484ceb4a6843ec16078038c10af

edc41f5362"

CCM encrypt and tag NIST VADT AES-128 #28 (P=24, N=13, A=27, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"fdf2b2c7fcb3789b4e90abe607dca2af":"d7aa4efa5d75195a400018bd38f7d8cd53fdffe88df1837f":"a69ddc66e63a3415f21009d53a":"c76846da496ed87b9c0f65c6266c9a822224acde9775efb186a4a5":"150d9a8b78d9c04239d66207a1f95021bbb1b7c70d7c354825d05e5a2e76a90f6fe489fd74cab2a3"

CCM
encrypt and tag NIST VADT AES-128 #29 (P=24, N=13, A=28, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"7d870d7e52d3053c65eefad47764cfeb":"109317556c21c969eda65a94176d7a11462c9ae18a865b6d":"37d888f4aa452d7bf217f5a529":"9610949f6d23d5b1f3989b2f4e524fab4f297a5bec8ddad4f16cb616":"4e6b967b1571c6d7b9e118b112b7ac949a4a175650316a242dd579cb0d201d22c86bbc7fbe47bd0d"

CCM encrypt and tag NIST VADT AES-128 #30 (P=24, N=13, A=29, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"8fcac40527c0e7ca8eaff265ca12c053":"78d1e96af8cebdcc7e7e2a4ddcfa34f6cf9a24fb85672ad7":"ae9f012fd9af60a400e20b1690":"9ce65598cd1f86afc9aaaf172809570cc306333c25523f863c6d0e0154":"9adb9a95a9379ad795d8d3ffd4e37a045160d6d727f974a6cb3b5151f327e65447e52c7525562c91"

CCM
encrypt and tag NIST VADT AES-128 #31 (P=24, N=13, A=30, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"ddf9f150cc3f1c15e8e773663c5b061c":"79d8841ab83279724ce35e1a8abd4e158168dcf388ab4c3d":"98c5036b7d54da9a1177105600":"20c5ab290e6d97f53c74121951f39ba865b3acc465fa3f0fb8a591622277":"d00d29396ffa9e691290d746527777bf96a851f306d4da0b1816df1e0e82bb7bc8105930ad6a2232"

CCM encrypt and tag NIST VADT AES-128 #32 (P=24, N=13, A=31, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"b1dc81d116d94f5eced526b37c004b95":"54390715b6e7c7bd51a234db059a51ba030cf22ee00b7277":"97c8f69fb91b17299461fd8d63":"f8b08aa83bed09ca342249b2cf9e2b45a89dcfb8711a120395e455921af481":"cb629994c3418a662a8cde1b5f4d99aa7df66e24c53dc6df11297930fd44c63675b7cca70671ef4d"

CCM encrypt and tag NIST VADT AES-128 #33 (P=24, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"5a33980e71e7d67fd6cf171454dc96e5":"a34dfa24847c365291ce1b54bcf8d9a75d861e5133cc3a74":"33ae68ebb8010c6b3da6b9cb29":"eca622a37570df619e10ebb18bebadb2f2b49c4d2b2ff715873bb672e30fc0ff":"7a60fa7ee8859e283cce378fb6b95522ab8b70efcdb0265f7c4b4fa597666b86dd1353e400f28864"

CCM

encrypt and tag NIST VADT AES-192 #1 (P=24, N=13, A=0, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"26511fb51fcfa75cb4b44da75a6e5a0eb8d9c8f3b906f886":"39f08a2af1d8da6212550639b91fb2573e39a8eb5d801de8":"15b369889699b6de1fa3ee73e5":"":"6342b8700edec97a960eb16e7cb1eb4412fb4e263ddd2206b090155d34a76c8324e5550c3ef426ed"

CCM encrypt and tag NIST VADT AES-192 #2 (P=24, N=13, A=1, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"9748798c0f3cc766795c8ce0e4c979c1930dfe7faefea84a":"100fa71462277d76ca81f2cfdb3d39d3894b0ca28074a0f0":"cdf4ba655acfe8e2134fa0542f":"67":"36e2415b4f888a6072f260d7e786d803be16f8b9cbee112d7ff74e3b05b7d7c13284573bd3e7e481"

CCM
encrypt and tag NIST VADT AES-192 #3 (P=24, N=13, A=2, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"393dcac5a28d77297946d7ab471ae03bd303ba3499e2ce26":"262f4ac988812500cb437f52f0c182148e85a0bec67a2736":"fe7329f343f6e726a90b11ae37":"1c8b":"e6d43f822ad168aa9c2e29c07f4592d7bbeb0203f418f3020ecdbc200be353112faf20e2be711908"

CCM encrypt and tag NIST VADT AES-192 #4 (P=24, N=13, A=3, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"a74abc4347e4be0acb0a73bb8f7d25c35bae13b77f80233a":"6372824bf416cd072a7ad0ae5f9f596c6127520c1b688ab4":"6a850e94940da8781159ba97ef":"a4490e":"b14a07bdc119d87611342c4c6935c5786ff1f9ae2eb49e6191c88a3cb4fbafcb8a4a157d587d7e39"

CCM encrypt and tag NIST VADT AES-192 #5 (P=24, N=13, A=4, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"df052e95aea3769a433ce4e4e800b8418649bbe8c6297eb0":"e8c1a89228d8212f75c136bab7923a89f9fea18e781cb836":"ba356d392c3f700f4f2706a4ca":"8ffc0e3d":"66b5d782323925e1bd0a8413a9a5a881356453d5df2cbeb199b2e1e803550dcdde55fd66ecb45edd"

CCM
encrypt and tag NIST VADT AES-192 #6 (P=24, N=13, A=5, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"16d345606a315ad2406abbcb43cd8cabe948107ba6d17a72":"d3bef460223c81e4579c9d1d463ac5e0881685de1420a411":"d4ef3e9e04f1b7f20ffc5a022e":"a468f08d07":"abb85db49a9b1c8724ecbc734cc8373bd20083cfa4007b1cfe4d3a3bb25f89f692884be230c6035c"

CCM encrypt and tag NIST VADT AES-192 #7 (P=24, N=13, A=6, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"1c476cfd7dd300d961fd3f24a6fe0e80742b00851676ca63":"6f3938932b5c1280311e892280d8a822a828a0be7fdb1bcd":"e300fc7a5b96806382c35af5b2":"28130f938c45":"df48662fe134e75a85abc2cece2c3b6236c88a70fa792e9beadc9601adf9fbdf4e3e94b395b0a332"

CCM encrypt and tag NIST VADT AES-192 #8 (P=24, N=13, A=7, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"79d1e38a70df1cf239be168833dcd0570bc8f37b3aa26c37":"83c24f3a77b83b4ef45277ba90225f3ba1722312f52b1a07":"8229d6d7e9e21fdc789bff5dcf":"076887d2abe9

00":"19d880f1d959a68f162de243d4a45747ace704613359b27218d1531a066de60a95d2924a6910e990"

CCM
 encrypt and tag NIST VADT AES-192 #9 (P=24, N=13, A=8, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"72e6cebdaf88205c4e74428664bc0d7eb4687a272217b7ca":"54bc7e3c227df4e83252a5848fea12dfdb2d14b9e67c1629":"3820db475c7cb04a0f74d8e449":"f427c47e10c45bb3":"91e7baff2b42af63e26c87ce6991af22422c1f82906858b1721961de5c768f4d19bd3034f44f08d2"

CCM encrypt and tag NIST VADT AES-192 #10 (P=24, N=13, A=9, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"39c03a0c8634047b1635348f284d3dc1e752ab40548eb337":"0662e63c88e963d3e0cf2c4653515ae4474a2c78ab0394c0":"9e2ea8eb7f56087ee506925648":"28d157f09a71da80dd":"01dcd4dd3b8c1369518136ce45e8bb9df565b0ad231a887b02ada34addf0aa2f4744ed2e07995491"

CCM
 encrypt and tag NIST VADT AES-192 #11 (P=24, N=13, A=10, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"e2a92ffbb0b5eb68cb82687f12449fae5167d375131b0b10":"048c9ba4597c3bb595bfd5048e5e9a1296f30e5c0118b177":"441ad5e1382e083a95224f395d":"2352648299b0413cb2ce":"25247a258e4ac0a988d8def60cc174a9d4578cd5346fb5150c96e8ab8774baa421f39c64a386c418"

CCM encrypt and tag NIST VADT AES-192 #12 (P=24, N=13, A=11, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"ef1ad3eb0bde7d4728389da2255d1f8a66ecb72e6f2f1ac4":"9f580cc6c62a05ce125c6bec109a48ca527ee26a64b14b68":"8e7d8a44244daa7df2b340993e":"521583c25eb4a3b2e46120":"ff0ff95bcb0bccd5e4aadd77ac6770f5013654eb3c6386fded2c87135861b43a99f258b6938f66e3"

CCM encrypt and tag NIST VADT AES-192 #13 (P=24, N=13, A=12, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"44cba20b7204ed85327c9c71c6fea00b47ce7bdde9dea490":"6333bde218b784ccd8370492f7c8c722f8ef143af66d71d7":"f3329154d8908f4e4a5b079992":"f1e0af185180d2eb63e50e37":"b9401a4927b34dc15e9193db00212f85f0c319781ec90e3b4484d93cb422cb564acc63d3d18e169c"

CCM
 encrypt and tag NIST VADT AES-192 #14 (P=24, N=13, A=13, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"b5f43f3ae38a6165f0f990abe9ee50cd9ad7e847a0a51731":"3726c1aaf85ee8099a7ebd3268700e07d4b3f292c65bba34":"13501aebda19a9bf1b5ffaa42a":"ead4c45ff9db54f9902a6de181":"fd80e88f07dad09eed5569a4f9bb65c42ef426dda40450119503d811701642143013f28ce384d912"

CCM encrypt and tag NIST VADT AES-192 #15 (P=24, N=13, A=14, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"13f179aa2a23bc90a85660306394940e9bb226ce3885ec01":"d3b36c6289ad6ae7c5d885fe83d62a76270689ce05fa3b48":"aaa52c63ca1f74a203d08c2078":"5cc924222692979a8e28ab1e0018":"bc4fcef401c2e1d1c335734ff23ea52c3474d2e6f31648a7f58649400ac9e825b038d67f0c2a6f1c"

CCM encrypt and tag NIST VADT AES-192 #16 (P=24, N=13, A=15, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"c1dfc48273d406a3a7b9176f80b2dc4e9a7f68134bab66d2":"67d9728a88f1fac3af43ed6d634ba902896bd226858697d9":"1ac53ba965cdaeeef7326a37e4":"39ba54a410a58a5d11615a2163cc3b":"360f0fc714994e3b59448b50cdd61d511b4f09e0e5fb5ac826a51fe5b9b598a17eb3da10f936813b"

CCM
encrypt and tag NIST VADT AES-192 #17 (P=24, N=13, A=16, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"d8a662ab8449bd037da0346a24565683a3bbbbd1800e3c1c":"61fdd10938557080191d13dd6c3002dd445d9af988029199":"166fb8d0e110124c09013e0568":"1c1c082eeb5b8548283d50cc2ace1c35":"23c05927502a4ee6e61e4e10552d49b020643eab476eeacc867601fe79a122a7817819655183283e"

CCM encrypt and tag NIST VADT AES-192 #18 (P=24, N=13, A=17, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"116f4855121d6aa53e8b8b43a2e23d468c8568c744f49de5":"1bd3b5db392402790be16e8d0a715453928f17f3384c13a7":"924322a3ef0c64412f460a91b2":"03c2d22a3bb08bbb96b2811ce4b1110a83":"ad736402626df0f9393fe4491eb812725ad39d6facf20b5b2f9340b0d48a17ae1cc71d7515e61ee9"

CCM
encrypt and tag NIST VADT AES-192 #19 (P=24, N=13, A=18, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"e67f3ba11282d61fe36e38cab7b559c2fd9cbe8bf7eb5863":"d7a954dae563b93385c02c82e0143b6c17ce3067d8b54120":"a727ed373886dd872859b92ccd":"68d199e8fced02b7aeba31aa94068a25d27a":"c6cfaa1f54d041089bd81f89197e57a53b2880cefc3f9d877e30b2bcc3f1ea9ec2b8f28bf0af4ecf"

CCM encrypt and tag NIST VADT AES-192 #20 (P=24, N=13, A=19, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"e0a29a2c7840cf9b41de49780b9ee92d646a4bfc5b9da74a":"344dc8b6bd66a1fbbe330a95af5dd2a8783dc264d6a9267d":"fc9fd876b1edded09f70b18824":"36e15baafa0002efbb4bb26503b7e3b79f6c68":"43b3b96aa5a54378f3bb573ffda3e154aa7f425fc3008175b60a77b9d38740356b544b1c0f259086"

CCM encrypt and tag NIST VADT AES-192 #21 (P=24, N=13, A=20, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"26d0a3a8509d97f81379d21981fe1a02c579121ab7356ca0":"37ab2a0b7b69942278e21032fc83eba6cdc34f5285a8b711":"8015c0f07a7acd4b1cbdd21b54":"093ed26ada5628cfb8cfc1391526b3bcc4af97d9":"a3a60b422eb070b499cf6da0a404b13a05cedda549c6b93e6ca0e07e04674f21a46df2659a5905fb"

CCM
encrypt and tag NIST VADT AES-192 #22 (P=24, N=13, A=21, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"aac60835c309d837aacc635931af95702a4784c214

283ebb":"e8610756528f75607b83926597ef515f4b32a8386437e6d4":"0e20602d4dc38baa1ebf94ded5":"796e55fbe7bed46d025599c258964a99574c523f6a":"e0a3d5f43e688ce104f4ae1a4fcd85500aa6b8fdbcd1b8d3003c0c3b7369e79339433e1754c0937f"

CCM encrypt and tag NIST VADT AES-192 #23 (P=24, N=13, A=22, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"671544bf2988056f7f9ccd526861391a27233793a23f811f":"576b069ae2713f53d2924c1fd68f786cb2eec68892f9e1be":"0a259148a1d081e0df381ecd0c":"61dafc237cb52f83ab773ba8a885462b6f77d4924611":"ce06b3d09b02921f290544032a081a7766612940048867281bb089af0245792c16e6320cf5ffa19e"

CCM
encrypt and tag NIST VADT AES-192 #24 (P=24, N=13, A=23, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"90e2c63b6e5394b1aeec03f95a9d13a01a7d4e9d58610786":"44dd098b1f869d670a8a841900c4bef023a1946a0c278354":"dada5465eb9b7229807a39e557":"f5629ca0eea589f6cf963d875a7d2efb656983f2dd2231":"6b38ca85450e05e7b9362ed7e6e291a130ff233b5a561cdef7ec84dd992fdf98514f845dac8f656e"

CCM encrypt and tag NIST VADT AES-192 #25 (P=24, N=13, A=24, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"13cdaaa4f5721c6d7e709cc048063cfb8b9d92e6425903e6":"d7c837971b973f5f651102bf8d032e7dcd10e306739a0d6c":"f97b532259babac5322e9d9a79":"ad6622279832502839a82348486d42e9b38626e8f06317c4":"4709600418f2839841e6d126359f6982bdb53acc7ff209635623d15b24184481eadc63bb8c878fc4"

CCM encrypt and tag NIST VADT AES-192 #26 (P=24, N=13, A=25, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"90851933d4d3257137984cdb9cba2ca737322dac4dbd64bc":"ba1785a149cb8b69a4e011c11a3ff06f6d7218f525ac81b5":"be02df3a840322df8d448c600c":"69a9dd9ac8be489c3a3f7f070bdaca10699171f66ab3da9351":"89ab2efefa8406336d9e2245199fbc9454f0ef650b9ed0f446c7246bd3130803bf8d703ef5bdf15c"

CCM
encrypt and tag NIST VADT AES-192 #27 (P=24, N=13, A=26, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"5c5d02c93faa74a848e5046fc52f236049e28cd8096dcac6":"b4da43ebfe9396b68f4689fba8837c68d0064841c6ddd4a7":"54cbf2889437673b8875a0f567":"09fc21ac4a1f43de29621cacf3ad84e055c6b220721af7ce33bb":"d40725397229021a18f3481e3a85f70445557bb2a85e4ae8101a34c777e918e16186fda05a386572"

CCM encrypt and tag NIST VADT AES-192 #28 (P=24, N=13, A=27, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"0234dae5bd7ae66c67ff0c1a3f1a191a0d7bceb451bc2b7d":"0f960a89a7e806f8709047cb7a2e7c4211ad724692c88a05":"16d345606a315ad2406abbcb43":"c37fdf7449fd7e943595d75e977089c623be0a3926e63fdbbfdf4a":"3907880d25f910eab12dd14e704d1b33ea7c453634d54da2a461f44dac1112ae3f9c65671a931d3e"

CCM
encrypt and tag NIST VADT AES-192 #29 (P=24, N=13, A=28, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"6351a67fd6daabd2fd49ee944dd41dd37301f958dd17fcc3":"0c0663dd69ccbffbbd0c8c2e9473d0354451ae7a20fa3695":"b8d517b033754058128d13d11a":"511c6924fa96db716f6b053b7a48aebdc1504145a56cd02d6be2590d":"19f2745df5007619c79c84d174e4521b942776478a0601d982c560fede4741e2fd3b54b3a48f3e38"

CCM encrypt and tag NIST VADT AES-192 #30 (P=24, N=13, A=29, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"9a5a9560baed3b8e0e90b92655d4e5f33889e5d7253d9f6c":"5bbe9c1fb2563e3e82999fe097b28da4dc6ff2e020f3b4f3":"c0049382cdd8646756d4e6bff5":"c95a86d52088a8b0107cc5b437a8938b2c9e74e46e2e03bb9bceecdbe3":"6d5401db42b5c48b79203b6ad82806d7460ac4c82ad0809b811020480e834f6fe55900a162a4e61a"

CCM encrypt
and tag NIST VADT AES-192 #31 (P=24, N=13, A=30, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"3e61094c80df0053e86d43fccf4e1d3ee2cdb862d3237b0a":"1fada8f4c7daea0d1c370184c169485b80a278708ed41451":"63f00b2488809fdc49ca5f05d5":"a08763ca936abdeece06467bef8c3c47c3a473636a039d4db540c867d3e3":"680dd22f16a1290bde42c9792dfa997aed24d5bd2265b6e095aa6b99d3f894d3790c2aa2dae1ba2c"

CCM encrypt and tag NIST VADT AES-192 #32 (P=24, N=13, A=31, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"b5664dd6ed435df006052f6ded74bb7ce9482ca9229886f7":"0b6de49b530703affc94010c2b793ddc6de0c44d48037ff2":"7a1649896f3e030c18f0205599":"c5f1a26351e53e6509c8bbbed03c42c23ad81c65fccec7ffa1cb494c7f1fc4":"56b02fea595cc24e798691ae905be3d466ca68ca744005dba260b5ea3b047020b73b5bafa17e5084"

CCM encrypt and tag NIST VADT AES-192 #33 (P=24, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"50925853a84a33ff392154e4e737efc18dcfc98f4d5235a9":"718f061e8b972a3adcf465d66c5b28e8661f080127f6722f":"809343e986f6ff47f54d4cac22":"d70aef3532bdc5293a3ebb11589ac1f801c9f93ea0d656e1d04068facf9f768b":"bad3b0e6772e9c4c9c631c095e259d99692292932efb72b8966e91a19617bb748f3495aa433585bb"

CCM
encrypt and tag NIST VADT AES-256 #1 (P=24, N=13, A=0, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"26511fb51fcfa75cb4b44da75a6e5a0eb8d9c8f3b906f886df3ba3e6da3a1389":"30d56ff2a25b83fee791110fcaea48e41db7c7f098a81000":"72a60f345a1978fb40f28a2fa4":"":"55f068c0bbba8b598013dd1841fd740fda2902322148ab5e935753e601b79db4ae730b6ae3500731"

CCM encrypt and tag NIST VADT AES-256 #2 (P=24, N=13, A=1, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"a4490ed6ab51dbfccd6f3702a857575dad44da3a27eaf31178abc97da60d1e4b":"1b5cc6b1651dec4bbbf5130343852e971c7ff1774100d9be":"26ceaf6e3b28190a17c4f0c3

78":"9e":"789bce069a725a96c484e64a9e54dcb7a7c268c85df47815a462ff2dd8ba44a381e1f6edab12b5a9"

CCM
encrypt and tag NIST VADT AES-256 #3 (P=24, N=13, A=2, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"df594db94ef8eca56a417afe946085eaed444c7cc648d07d58132e6cb5bc2bc3":"f4d7978fad36223623ccb5bb18a7373cba8a6e3b1c921259":"c1ad812bf2bbb2cdaee4636ee7":"c0c3":"bea778540a90033b2c0d087e3cc447711ea25f7eea96855506ec97f23bd6ea97834f92f7263c3195"

CCM encrypt and tag NIST VADT AES-256 #4 (P=24, N=13, A=3, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"d98193ab2a465e3fcd85651aaeca18b8e91489b73b7c7e93b518c4b5b81fc6ac":"edba7d6312144e90ec9eaace7576045a46e553dcb8ee5a98":"2247dc7e2674e9e0a63fe70613":"4dc2f4":"44b9ea727c847336fd739ad11f4b906b292edb810462f06ef59626ad5cdac2e4d4cb07b538a1fd8f"

CCM encrypt and tag NIST VADT AES-256 #5 (P=24, N=13, A=4, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"45c8afd7373cb0f6b092af3a633d9fd97c4ca378e19d75f9b74d089429726c29":"0b92adbb251dc29a67f0bb97f8e7160862b6c4e843d07fd9":"fdb1fa230ae0b172ff98fc7496":"270981af":"274e2faea3271ea6fa0494c1951f115b5491a893056c3ee4c76fc350e585277e373e9119bf9595cb"

CCM
encrypt and tag NIST VADT AES-256 #6 (P=24, N=13, A=5, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"a2e6bf39efd1ceddc92b4333ed92d65efeea6c031ca345adb93a7770a8039bcd":"d822f84b023f12ea9e3ce16b904278e4aaab5e11c2c23f3f":"693cbb46bc8366086ec7cd7776":"3ba11282d6":"9f91fd2f6472e33b02b1eabb9d6655729d44c44dad6b3883fe0667bcc5806b225224b04ade8b21c1"

CCM encrypt and tag NIST VADT AES-256 #7 (P=24, N=13, A=6, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"c5a850167a5bfdf56636ce9e56e2952855504e35cc4f5d24ee5e168853be82d8":"e758796d7db73bccb1697c42df691ac57974b40ca9186a43":"c45b165477e8bfa9ca3a1cd3ca":"4759557e9bab":"93ad58bd5f4f77ac4f92b0ae16c62489e4074c7f152e2ed8a88179e0d32f4928eff13b4ce2873338"

CCM encrypt and tag NIST VADT AES-256 #8 (P=24, N=13, A=7, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"ae8f93c3efe38e2af07e256961dd33028faa0716e5320a7ab319a10d2f4c5548":"bc9ca92a9c9919e39095d3e53fb148694620ae61227e0069":"6333bde218b784ccd8370492f7":"0b1fabdf2a4107":"45811b0c8f754bf03950e520cd4afc81c2e3eb8a11f4fd386d5a6e4b1fbee15d35939c721004502e"

CCM
encrypt and tag NIST VADT AES-256 #9 (P=24, N=13, A=8, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"548c2d1eb7d91e003633d4d9ff199e4a8447180edd89ac7867d25a1db288b5ce":"49fd5cbe4aff89dc3b8718f9ce545d612cbbebb289ecbf42":"23b205bd6ff8ed0bab0c989

99c":"a6601111cd92c943":"3cfc6211e359ae322802fc9566f377b0dfe17d1dfe0878ebf2a9047e37cc0be1fab0006af8db8dc4"

CCM encrypt and tag NIST VADT AES-256 #10 (P=24, N=13, A=9, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"aab793e377a12484dbdd74c9b3a85c74c286e1cc498663fbd7c718b5633bb91a":"7c0889854658d3408c5d8043aad2f4ae4a89449a36f8a3b8":"10022cddb323e88b3c08f95a0f":"82b8c736037ce2f2e8":"1044250f58857c69f72b5d3454d43949e5c02b3822970b280de1a3f7fc5d06cc30f06075f5504ed7"

CCM
encrypt and tag NIST VADT AES-256 #11 (P=24, N=13, A=10, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"06ac39896073a44283611a66ccab067e2dd2faa8da82ff9a45bb29e54d2e6e77":"3216dce3b8b1ce0e79e40fffcac728ab191aaaf319d971d3":"6c7942c9819cf69b817bfcdb0a":"215e2a6c24325340fdec":"c5b3b50ed8a7b7b96b02ba9464b6a2ff80e90548605699a63d70e6dffb31a376a1eb7f94526dca48"

CCM encrypt and tag NIST VADT AES-256 #12 (P=24, N=13, A=11, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"50412c6444bcf9829506ab019e98234af1541061557412740bc120b456052763":"6cdbd63f6d591f59776f828533b28e2453a214d1d0dd8a39":"85684f94c3702c5d870310166d":"f706a3e09df95d3e21d2e0":"8c8b4ae854a5d5c265b25e3b54bded9444cc454b3e0e6a24d6c05eaf406a5ebd578e19edd5227380"

CCM encrypt and tag NIST VADT AES-256 #13 (P=24, N=13, A=12, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"8a56588fe5e125237b6cdc30f940b8d88b2863ec501a0cb00b1abade1b5ce0ed":"c825952293e434ea866db558aaf486ef09a92bf366988f71":"d80210b9f9776ea36dc0e0a787":"e4296d1c8cf4ffc4b2635135":"b8b3b15fdf6a4a0b5abc313afc769e4e8413bd887552583ede3ed995d1b70561c8e28a7b1a7e3dc8"

CCM
encrypt and tag NIST VADT AES-256 #14 (P=24, N=13, A=13, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"a4cc7e1c90f8684e6a5f95e6898ab4e3c194cb46e196d8228062b9f3fa744930":"10d4cff95ef490923c9e0906880729d4d05412e7675cce76":"cdc2712e51c7f333d6bad78eee":"569c56b27268d3db54e728aac0":"be3ce3e9dc72499839a98ae52abb17415e8547687e8a3c7b8aaaac20d4c9276f2851cbba2b04d185"

CCM encrypt and tag NIST VADT AES-256 #15 (P=24, N=13, A=14, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"347e12eec56e95aafcc7d25bf10fc756b4e42bc2e43da7f97df24331f27f1f5c":"ca88dddfc876a12f45f19562bc9ca250f43267ab251a7f34":"b8d517b033754058128d13d11a":"511c6924fa96db716f6b053b7a48":"eeedcfa8f5b5b48c1d7e277526eecb7294213b9f5785167ae949b93003dfe63c95c1d49edfb4de3f"

CCM

encrypt and tag NIST VADT AES-256 #16 (P=24, N=13, A=15, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"520902aa27c16dee112812b2e685aa203aeb8b8633bd1bfc99728a482d96c1fe":"533fee7d2c7740db55770e48cb1b541d990ea3f8f08ed1a6":"ddf50502f414c1bf24888f1328":"22b4f8f1aac02a9b2ef785d0ff6f93":"fc867b319e0e4ab45ec518a1b5dcec4f29982173f3abfd4d8a8f8d14d2bdac84c3737cfbd75b7c0b"

CCM encrypt and tag NIST VADT AES-256 #17 (P=24, N=13, A=16, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"57da1c2704219ed59abfdf04743a9a93c87a63d471818de0f1564b2db6421562":"ddc3c1aa73fb6de92bb4db138e26f3c2e0543ab4f5924871":"4b60a47b7e90f622fa0bf803e1":"0ae8c012ff39753510df3ee80707e4e2":"daa8256d4753fdf9cfef876295badaba89b45cc497f54d220ec2c6fb687753bca4580adc6aa2f296"

CCM encrypt and tag NIST VADT AES-256 #18 (P=24, N=13, A=17, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"9267ebc99ccf648b146cba3c251187e24a9947d806ceb0ced6894211641a1e0d":"967daf12f16f166b7b5038f83a1cf0b980f5abf4c7746f2a":"9b7298950280e8762ecdc9bbe4":"5824689453bc406bf891b85e4576e38fe8":"7cfe2a7a54306eb8d8a63d3d1ae86794f9a2c22198b2cb4f10ca926f1a430c08c12e23db3d913e93"

CCM
encrypt and tag NIST VADT AES-256 #19 (P=24, N=13, A=18, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"7a855e1690ee638de01db43b37401dcd569c1ae03dc73dd0a917d0cadb5abc29":"33ae68ebb8010c6b3da6b9cb29fe9f8bd09b59ec39f4ce4b":"8f160a873a1166c8b32bccbba7":"72674aca7eba2fc0eeafbd143c2c4d8aa6c8":"b22afdf4f12c43ec23e01ac1215a3f5286059211207e957057e9a9203da74387a9468f8af5e27547"

CCM encrypt and tag NIST VADT AES-256 #20 (P=24, N=13, A=19, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"0ebdc6ddb4c502725dd6ee8da95d56a0d1044b4694d6ba8475a4434f23a8474f":"c7360282c85484a5a33ab1c68dd70873ab4e74ffd4a62cd5":"fb717a8c82114477253acc14f6":"41e9d65632f74f449a6842d5e6c4a86ef83791":"2e961b3a2fa1609a4e6fd04bff6ac5e306ae2638706f997b42be2e2ba05c54b619850db5c9d684fe"

CCM
encrypt and tag NIST VADT AES-256 #21 (P=24, N=13, A=20, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"2ff64bbec197a63315c2f328dcb4837d0cdc21a5d6f89ff1d97cb51195330cd8":"4a17522da707b4b2587a0ae367a2cd2831bb593a18ef442a":"a235f8ee3de9896b71910ac02c":"2b411bea57b51d10a4d2fb17ef0f204aa53cf112":"1bf122798bd8ee8e73391d589bd046a294d1615794e69cb9e6f3ba30143acbc3a1c1c6ec74333107"

CCM encrypt and tag NIST VADT AES-256 #22 (P=24, N=13, A=21, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"24e9f08a9a007f9976919e10dc432002e2e078a339677f00105c72ed35633a3f":"d3416a81b4246eb0bf8119a72a886bbc0ac9449c69f71d2f":"15977424eeec0ec7f647e6c

798":"2d838eb51a4bc69a001a18adf2084a680f02a3c5fc":"e001a8fae390dc5d672cdd18f86a1f728158ec83a002050def9af5679edbcbb7db20ab6af30698db"

CCM encrypt and tag NIST VADT
AES-256 #23 (P=24, N=13, A=22, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"0ec1b22b8df05dc92135d2dfbefed8ea81458f5ea1b801e8a218faf6cbdf1a79":"2f59d94d4ab8eeb84c2a6fefb7fb0a3ac059c1e1a65ae34a":"97ebcb8575bb58260208d5c227":"a2f6337f86dd00d1a58448851e95d8c9bace4a5c8710":"7ca0b1dbe34b0391e524b868b0af08b3e096917664d6aa2cabc1f9d0132394149c9062b74b82f04b"

CCM encrypt and tag NIST VADT AES-256 #24 (P=24, N=13, A=23, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"0875020959ed969cfb38636d1d5aabce9658b00171a7614ea9e5395331c7659c":"065ef9eeafbe077c1c7049f43eb0d8999708e8609f214d5c":"451101250ec6f26652249d59dc":"7cc9c51b69f98a06391ab32742fb6365e15106c811fe8a":"990065322a438e136860f7b019807e9feff52a642bf3d44a9163fa7a867f04cab6f52dc250070f31"

CCM encrypt and tag NIST VADT AES-256 #25 (P=24, N=13, A=24, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"ef4c1d2314e671f666cc6667660f1438a293208c7cc29b412d81277f0a635c91":"c99c3e79125b6fd95e737326a842424eb6c6ecea4c0475c4":"50b23b052922366c25dd40e348":"cd0522ebe1fed82465277d1c10ae9316a98b4469be63b180":"76df4be4ec8373864399acda11294b220b9f7c3a7d2b3660b25764e40ac6a171e7e6bab4fdee4288"

CCM
encrypt and tag NIST VADT AES-256 #26 (P=24, N=13, A=25, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"8544808e8fbf8c3a5e1d4ca751d4b603af9fe119eabc6923205815e0e748b7e7":"617d54fc6a23601c79e3984f93bfc2d151fde420863206b3":"b44a58724596b4d8dea827c1a0":"f5b2c88f5232c37273b1e66aa31cfa7201e33c21d60054d025":"57b3414db48982c6567265e1e0173bf38fdfaffe4461fbebc1411af83237c0f9eb0bfe8ed914da66"

CCM encrypt and tag NIST VADT AES-256 #27 (P=24, N=13, A=26, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"e19eaddd9f1574447e7e6525f7fd67e3b42807e44fbb60e75d8c3e98abc18361":"b3b0de10b7c0996662f1b064e04e528b7d85ca1166985d33":"a8c459ce0223358826fb1ec0f0":"ef88f4393d6c1e7b7be55a12144209ee051bb779e440432721ef":"d63e6082c95c6c5ff2bc0771321a4f883ef61cff7b99e0ea8a20a1abe7c842ebc08c8c81a2743c81"

CCM
encrypt and tag NIST VADT AES-256 #28 (P=24, N=13, A=27, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"9498f02e50487cfbda1ce6459e241233bd4c4cb10281dcb51915dbc7fb6545c0":"0d16cc69caa9f19b88b05e151b3d26accd018ca4a5786a80":"e3bd4bc3a60cddd26c20aa8636":"70cfcb828d483216b46c3cd22e2f9ee879e9e3059b566179b6e16c":"f1c4bedb8d6f91676881daa37656a7e6402f472735b04a0f1f8332f4236437737438e7aa1b5100c7"

CCM encrypt and tag NIST VADT AES-256 #29 (P=24, N=13, A=28, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"3ac7d5bc4698c021e49a685cd71057e09821633957d1d59c3c30cbc3f2d1dbf8":"89198d3acc39b950f0d411119c478c60b2422ffe7e26e00b":"54c8ff5459702aac058bb3be04":"ecbd7091732e49c0f4bda2e63235ea43bbf8c8730f955f9c049dd1ec":"7717b8e4447afcea1eeebf3e39ffdab2f52828e7931ef27e475acd27900478f09fec1f479ab3a7c8"

CCM encrypt and tag NIST VADT AES-256 #30 (P=24,
N=13, A=29, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"948882c3667caa81c9b900996e3d591e6fcb3d08333eeb29911e9c6338710c17":"8b9130b0c3c15366831bbb19f377e3209a8dbf7619cd09bd":"43b0aca2f0a9030f90559fa6d3":"a516ca8405e5c8854e667921b5c5e1968bdd052915b55ac9984b7eefb3":"4646b2acdeb11174171da23999cd54e297daa32bbc13d30512e57c576b315f48c11877178389aaa0"

CCM encrypt and tag NIST VADT AES-256 #31 (P=24, N=13, A=30, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"3bf52cc5ee86b9a0190f390a5c0366a560b557000dbe5115fd9ee11630a62769":"094b538110495e938b08cf748a6bcf3e0c80ff9c66570237":"f9fbd02f28ecc929d369182752":"ebf0b3e3199a5c3773c761c725c7600add5f9d8321c9f8e5e5fd1c7a5d2f":"4d8b53016fc8bc9677184c0fa15bbd3d671b9366d82ecb67f8562eadcdcbcdbad1299bea1523f5d2"

CCM encrypt and tag NIST VADT AES-256 #32 (P=24, N=13, A=31, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"e45bb1730d0d539aab3805350ac986540de9f0f6c239ee70395c291397b70309":"bc8b3bc48c7a88c9fafde258b6ccaa9d4f0d018703d63871":"d5c7824af715bb7822b6b340fe":"860f4a09ad8b3d345c2aa18ffb803f0bc3b734a4d047a1437701a5e3d95288":"95f083ad6bbaee6ab540fe023858f8baf25e333fd3e89c00e678a392d228b210dc5c991905dacf3f"

CCM
encrypt and tag NIST VADT AES-256 #33 (P=24, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"2e6e34070caf1b8820ed39edfa83459abe1c15a1827f1c39f7ac316c4c27910f":"771a7baa9cf83aa253349f6475d5e74dba4525307b022ba7":"c49ccef869bb86d21932cb443b":"d37e35d7cdccd9824a1ae4c787819735e4af798a3beb49d4705336d6496853ad":"eebac2475004970071dfa2cfb855c4e78b1add8dcbccfc0bd6b14027324b657a56263df148665393"

CCM auth decrypt tag NIST DVPT AES-128 #1 (P=0, N=7, A=0, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"4ae701103c63deca5b5a3939d7d05992":"02209f55":"5a8aa485c316e9":"":4:""

CCM auth decrypt tag NIST DVPT AES-128 #2 (P=0, N=7, A=0, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"4ae701103c63deca5b5a3939d7d05992":"9a04c241":"3796cf51b87266":"":4:"FAIL"

CCM

auth decrypt tag NIST DVPT AES-128 #3 (P=0, N=7, A=0, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"4bb3c4a4f893ad8c9bdc833c325d62b3":"75d582db43ce9b13ab4b6f7f14341330":"5a8aa485c316e9":"":16:""

CCM auth decrypt tag NIST DVPT AES-128 #4 (P=0, N=7, A=0, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"4bb3c4a4f893ad8c9bdc833c325d62b3":"3a65e03af37b81d05acc7ec1bc39deb0":"3796cf51b87266":"":16:"FAIL"

CCM auth decrypt tag NIST DVPT AES-128 #5 (P=0, N=13, A=0, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"4bb3c4a4f893ad8c9bdc833c325d62b3":"90156f3f":"5a8aa485c316e9403aff859fbb":"":4:""

CCM auth decrypt tag NIST DVPT AES-128 #6 (P=0, N=13, A=0, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"4bb3c4a4f893ad8c9bdc833c325d62b3":"88909016":"a16a2e741f1cd9717285b6d882":"":4:"FAIL"

CCM
auth decrypt tag NIST DVPT AES-128 #7 (P=0, N=13, A=0, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"19ebfde2d5468ba0a3031bde629b11fd":"fb04dc5a44c6bb000f2440f5154364b4":"5a8aa485c316e9403aff859fbb":"":16:""

CCM auth decrypt tag NIST DVPT AES-128 #8 (P=0, N=13, A=0, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"19ebfde2d5468ba0a3031bde629b11fd":"5447075bf42a59b91f08064738b015ab":"a16a2e741f1cd9717285b6d882":"":16:"FAIL"

CCM auth decrypt tag NIST DVPT AES-128 #9 (P=24, N=7, A=0, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"19ebfde2d5468ba0a3031bde629b11fd":"a90e8ea44085ced791b2fdb7fd44b5cf0bd7d27718029bb703e1fa6b":"5a8aa485c316e9":"":4:"3796cf51b8726652a4204733b8fbb047cf00fb91a9837e22"

CCM auth decrypt tag NIST DVPT AES-128 #10 (P=24, N=7, A=0, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"19ebfde2d5468ba0a3031bde629b11fd":"50aafe0578c115c4a8e126ff7b3ccb64dce8ccaa8ceda69f23e5d81c":"31f8fa25827d48":"":4:"FAIL"

CCM
auth decrypt tag NIST DVPT AES-128 #11 (P=24, N=7, A=0, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"197afb02ffbd8f699dacae87094d5243":"24ab9eeb0e5508cae80074f1070ee188a637171860881f1f2d9a3fbc210595b7b8b1b41523111a8e":"5a8aa485c316e9":"":16:"3796cf51b8726652a4204733b8fbb047cf00fb91a9837e22"

CCM auth decrypt tag NIST DVPT AES-128 #12 (P=24, N=7, A=0, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"197afb02ffbd8f699dacae87094d5243":"7ebfda6fa5da1dbffd82dc29b875798fbcef8ba0084fbd2463af747cc88a001fa94e060290f209c4":"31f8fa25827d48":"":16:"FAIL"

CCM auth decrypt tag NIST DVPT AES-128 #13 (P=24, N=13, A=0, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"197afb02ffbd8f699dacae87094d5243":"4a550134f94455979ec4bf89ad2bd80d25a77ae94e456134a3e138b9":"5a8aa485c316e9403aff859fbb":"":4:"a16a2e741f1cd9717285b6d882c1fc53655e9773761ad697"

CCM
auth decrypt tag NIST DVPT AES-128 #14 (P=24, N=13, A=0, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"197afb02ffbd8f699dacae87094d5243":"118ec53dd1bfbe52d5b9fe5dfebecf2ee674ec983eada654091a5ae9":"49004912fdd7269279b1f06a89":"":4:"FAIL"

CCM auth decrypt tag NIST DVPT AES-128 #15 (P=24, N=13, A=0, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"90929a4b0ac65b350ad1591611fe4829":"4bfe4e35784f0a65b545477e5e2f4bae0e1e6fa717eaf2cb6a9a970b9beb2ac1bd4fd62168f8378a":"5a8aa485c316e9403aff859fbb":"":16:"a16a2e741f1cd9717285b6d882c1fc53655e9773761ad697"

CCM auth decrypt tag NIST DVPT AES-128 #16 (P=24, N=13, A=0, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"90929a4b0ac65b350ad1591611fe4829":"0c56a503aa2c12e87450d45a7b714db980fd348f327c0065a65666144994bad0c8195bcb4ade1337":"49004912fdd7269279b1f06a89":"":16:"FAIL"

CCM auth decrypt tag NIST DVPT AES-128 #17 (P=0, N=7,
A=32, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"90929a4b0ac65b350ad1591611fe4829":"782e4318":"5a8aa485c316e9":"3796cf51b8726652a4204733b8fbb047cf00fb91a9837e22ec22b1a268f88e2c":4:""

CCM auth decrypt tag NIST DVPT AES-128 #18 (P=0, N=7, A=32, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"90929a4b0ac65b350ad1591611fe4829":"a04f270a":"a265480ca88d5f":"a2248a882ecbf850daf91933a389e78e81623d233dfd47bf8321361a38f138fe":4:"FAIL"

CCM auth decrypt tag NIST DVPT AES-128 #19 (P=0, N=7, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"6a798d7c5e1a72b43e20ad5c7b08567b":"41b476013f45e4a781f253a6f3b1e530":"5a8aa485c316e9":"3796cf51b8726652a4204733b8fbb047cf00fb91a9837e22ec22b1a268f88e2c":16:""

CCM auth decrypt tag NIST DVPT AES-128 #20 (P=0, N=7, A=32, T=16)

depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"6a798d7c5e1a72b43e20ad5c7b08567b":"f9f018fcd12
5822616083fffebc4c8e6":"a265480ca88d5f":"a2248a882ecbf850daf91933a389e78e81623d233dfd47bf8321361a38f
138fe":16:"FAIL"

CCM
 auth decrypt tag NIST DVPT AES-128 #21 (P=0, N=13, A=32, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"6a798d7c5e1a72b43e20ad5c7b08567b":"9f69f24f":"5
a8aa485c316e9403aff859fbb":"a16a2e741f1cd9717285b6d882c1fc53655e9773761ad697a7ee6410184c7982":4:""

CCM auth decrypt tag NIST DVPT AES-128 #22 (P=0, N=13, A=32, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"6a798d7c5e1a72b43e20ad5c7b08567b":"e17afaa4":"8
739b4bea1a099fe547499cbc6":"f6107696edb332b2ea059d8860fee26be42e5e12e1a4f79a8d0eafce1b2278a7":4:"FA
IL"

CCM auth decrypt tag NIST DVPT AES-128 #23 (P=0, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"f9fdca4ac64fe7f014de0f43039c7571":"1859ac36a40a
6b28b34266253627797a":"5a8aa485c316e9403aff859fbb":"a16a2e741f1cd9717285b6d882c1fc53655e9773761ad6
97a7ee6410184c7982":16:""

CCM auth decrypt
 tag NIST DVPT AES-128 #24 (P=0, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"f9fdca4ac64fe7f014de0f43039c7571":"edf8b46eb69ac
0044116019dec183072":"8739b4bea1a099fe547499cbc6":"f6107696edb332b2ea059d8860fee26be42e5e12e1a4f79
a8d0eafce1b2278a7":16:"FAIL"

CCM auth decrypt tag NIST DVPT AES-128 #25 (P=24, N=7, A=32, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"f9fdca4ac64fe7f014de0f43039c7571":"6be31860ca27
1ef448de8f8d8b39346daf4b81d7e92d65b338f125fa":"5a8aa485c316e9":"3796cf51b8726652a4204733b8fbb047cf0
0fb91a9837e22ec22b1a268f88e2c":4:"a265480ca88d5f536db0dc6abc40faf0d05be7a966977768"

CCM auth decrypt tag NIST DVPT AES-128 #26 (P=24, N=7, A=32, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"f9fdca4ac64fe7f014de0f43039c7571":"4cc57a9927a6
bc401441870d3193bf89ebd163f5c01501c728a66b69":"fdd2d6f503c915":"5b92394f21ddc3ad49d9b0881b829a593
5cb3a4d23e292a62fb66b5e7ab7020e":4:"FAIL"

CCM
 auth decrypt tag NIST DVPT AES-128 #27 (P=24, N=7, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"a7aa635ea51b0bb20a092bd5573e728c":"b351ab96b2e
45515254558d5212673ee6c776d42dbca3b512cf3a20b7fd7c49e6e79bef475c2906f":"5a8aa485c316e9":"3796cf51b
8726652a4204733b8fbb047cf00fb91a9837e22ec22b1a268f88e2c":16:"a265480ca88d5f536db0dc6abc40faf0d05be7

a966977768"

CCM auth decrypt tag NIST DVPT AES-128 #28 (P=24, N=7, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"a7aa635ea51b0bb20a092bd5573e728c":"df1a5285caa41b4bb47f6e5ceceba4e82721828d68427a3081d18ca149d6766bfaccec88f194eb5b":"fdd2d6f503c915":"5b92394f21ddc3ad49d9b0881b829a5935cb3a4d23e292a62fb66b5e7ab7020e":16:"FAIL"

CCM auth decrypt tag NIST DVPT AES-128 #29 (P=24, N=13, A=32, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"a7aa635ea51b0bb20a092bd5573e728c":"934f893824e880f743d196b22d1f340a52608155087bd28ac25e5329":"5a8aa485c316e9403aff859fbb":"a16a2e741f1cd9717285b6d882c1fc53655e9773761ad697a7ee6410184c7982":4:"8739b4bea1a099fe547499cbc6d1b13d849b8084c9b6acc5"

CCM
auth decrypt tag NIST DVPT AES-128 #30 (P=24, N=13, A=32, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"a7aa635ea51b0bb20a092bd5573e728c":"f43ba9d834ad85dfab3f1c0c27c3441fe4e411a38a261a6559b3b3ee":"0812757ad0cc4d17c4cfe7a642":"ec6c44a7e94e51a3ca6dee229098391575ec7213c85267fbf7492fdbeee61b10":4:"FAIL"

CCM auth decrypt tag NIST DVPT AES-128 #31 (P=24, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"26511fb51fcfa75cb4b44da75a6e5a0e":"50038b5fdd364ee747b70d00bd36840ece4ea19998123375c0a458bfcafa3b2609afe0f825cbf503":"5a8aa485c316e9403aff859fbb":"a16a2e741f1cd9717285b6d882c1fc53655e9773761ad697a7ee6410184c7982":16:"8739b4bea1a099fe547499cbc6d1b13d849b8084c9b6acc5"

CCM auth decrypt tag NIST DVPT AES-128 #32 (P=24, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"26511fb51fcfa75cb4b44da75a6e5a0e":"78ed8ff6b5a1255d0fbd0a719a9c27b059ff5f83d0c4962c390042ba8bb5f6798dab01c5afad7306":"0812757ad0cc4d17c4cfe7a642":"ec6c44a7e94e51a3ca6dee229098391575ec7213c85267fbf7492fdbeee61b10":16:"FAIL"

CCM
auth decrypt tag NIST DVPT AES-192 #1 (P=0, N=7, A=0, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"c98ad7f38b2c7e970c9b965ec87a08208384718f78206c6c":"9d4b7f3b":"5a8aa485c316e9":"":4:""

CCM auth decrypt tag NIST DVPT AES-192 #2 (P=0, N=7, A=0, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"c98ad7f38b2c7e970c9b965ec87a08208384718f78206c6c":"80745de9":"3796cf51b87266":"":4:"FAIL"

CCM auth decrypt tag NIST DVPT AES-192 #3 (P=0, N=7, A=0, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"4bb3c4a4f893ad8c9bdc833c325d62b3d3ad1bccf9282a

65":"17223038fa99d53681ca1beabe78d1b4":"5a8aa485c316e9":"":16:""

CCM auth decrypt tag NIST DVPT AES-192 #4 (P=0, N=7, A=0,
T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"4bb3c4a4f893ad8c9bdc833c325d62b3d3ad1bccf9282a65":"d0e1eeef4d2a264536bb1c2c1bde7c35":"3796cf51b87266":"":16:"FAIL"

CCM auth decrypt tag NIST DVPT AES-192 #5 (P=0, N=13, A=0, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"4bb3c4a4f893ad8c9bdc833c325d62b3d3ad1bccf9282a65":"fe69ed84":"5a8aa485c316e9403aff859fbb":"":4:""

CCM auth decrypt tag NIST DVPT AES-192 #6 (P=0, N=13, A=0, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"4bb3c4a4f893ad8c9bdc833c325d62b3d3ad1bccf9282a65":"db7ffc82":"a16a2e741f1cd9717285b6d882":"":4:"FAIL"

CCM auth decrypt tag NIST DVPT AES-192 #7 (P=0, N=13, A=0, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"19ebfde2d5468ba0a3031bde629b11fd4094afcb205393fa":"0c66a8e547ed4f8c2c9a9a1eb5d455b9":"5a8aa485c316e9403aff859fbb":"":16:""

CCM auth decrypt tag NIST DVPT AES-192 #8 (P=0, N=13, A=0, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"19ebfde2d5468ba0a3031bde629b11fd4094afcb205393fa":"38757b3a61a4dc97ca3ab88bf1240695":"a16a2e741f1cd9717285b6d882":"":16:"FAIL"

CCM
auth decrypt tag NIST DVPT AES-192 #9 (P=24, N=7, A=0, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"19ebfde2d5468ba0a3031bde629b11fd4094afcb205393fa":"411986d04d6463100bff03f7d0bde7ea2c3488784378138cddc93a54":"5a8aa485c316e9":"":4:"3796cf51b8726652a4204733b8fbb047cf00fb91a9837e22"

CCM auth decrypt tag NIST DVPT AES-192 #10 (P=24, N=7, A=0, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"19ebfde2d5468ba0a3031bde629b11fd4094afcb205393fa":"32b649ab56162e55d4148a1292d6a225a988eb1308298273b6889036":"31f8fa25827d48":"":4:"FAIL"

CCM auth decrypt tag NIST DVPT AES-192 #11 (P=24, N=7, A=0, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"197afb02ffbd8f699dacae87094d524324576b99844f75e1":"cba4b4aeb85f0492fd8d905c4a6d8233139833373ef188a8c5a5ebecf7ac8607fe412189e83d9d20":"5a8aa485c316e9":"":16:"3796cf51b8726652a4204733b8fbb047cf00fb91a9837e22"

CCM

auth decrypt tag NIST DVPT AES-192 #12 (P=24, N=7, A=0, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"197afb02ffbd8f699dacae87094d524324576b99844f75e1":"ca62713728b5c9d652504b0ae8fd4fee5d297ee6a8d19cb6e699f15f14d34dcaf9ba8ed4b877c97d":"31f8fa25827d48":"":16:"FAIL"

CCM auth decrypt tag NIST DVPT AES-192 #13 (P=24, N=13, A=0, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"197afb02ffbd8f699dacae87094d524324576b99844f75e1":"042653c674ef2a90f7fb11d30848e530ae59478f1051633a34fad277":"5a8aa485c316e9403aff859fbb":"":4:"a16a2e741f1cd9717285b6d882c1fc53655e9773761ad697"

CCM auth decrypt tag NIST DVPT AES-192 #14 (P=24, N=13, A=0, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"197afb02ffbd8f699dacae87094d524324576b99844f75e1":"1902d9769a7ba3d3268e1257395c8c2e5f98eef295dcbfa5a35df775":"49004912fdd7269279b1f06a89":"":4:"FAIL"

CCM
auth decrypt tag NIST DVPT AES-192 #15 (P=24, N=13, A=0, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"90929a4b0ac65b350ad1591611fe48297e03956f6083e451":"a5b7d8cca2069908d1ed88e6a9fe2c9bede3131dad54671ea7ade30a07d185692ab0ebdf4c78cf7a":"5a8aa485c316e9403aff859fbb":"":16:"a16a2e741f1cd9717285b6d882c1fc53655e9773761ad697"

CCM auth decrypt tag NIST DVPT AES-192 #16 (P=24, N=13, A=0, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"90929a4b0ac65b350ad1591611fe48297e03956f6083e451":"9a98617fb97a0dfe466be692272dcdaec1c5443a3b51312ef042c86363cc05afb98c66e16be8a445":"49004912fdd7269279b1f06a89":"":16:"FAIL"

CCM auth decrypt tag NIST DVPT AES-192 #17 (P=0, N=7, A=32, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"90929a4b0ac65b350ad1591611fe48297e03956f6083e451":"1d089a5f":"5a8aa485c316e9":"3796cf51b8726652a4204733b8fbb047cf00fb91a9837e22ec22b1a268f88e2c":4:""

CCM
auth decrypt tag NIST DVPT AES-192 #18 (P=0, N=7, A=32, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"90929a4b0ac65b350ad1591611fe48297e03956f6083e451":"2f46022a":"a265480ca88d5f":"a2248a882ecbf850daf91933a389e78e81623d233dfd47bf8321361a38f138fe":4:"FAIL"

CCM auth decrypt tag NIST DVPT AES-192 #19 (P=0, N=7, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"6a798d7c5e1a72b43e20ad5c7b08567b12ab744b61c070e2":"5280a2137fee3deefcfe9b63a1199fb3":"5a8aa485c316e9":"3796cf51b8726652a4204733b8fbb047cf00fb91a9

837e22ec22b1a268f88e2c":16:""

CCM auth decrypt tag NIST DVPT AES-192 #20 (P=0, N=7, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"6a798d7c5e1a72b43e20ad5c7b08567b12ab744b61c070e2":"d40a7318c5f2d82f838c0beeefe0d598":"a265480ca88d5f":"a2248a882ecbf850daf91933a389e78e81623d233dfd47bf8321361a38f138fe":16:"FAIL"

CCM auth decrypt tag NIST DVPT AES-192
#21 (P=0, N=13, A=32, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"6a798d7c5e1a72b43e20ad5c7b08567b12ab744b61c070e2":"5e0eaebd":"5a8aa485c316e9403aff859fbb":"a16a2e741f1cd9717285b6d882c1fc53655e9773761ad697a7ee6410184c7982":4:""

CCM auth decrypt tag NIST DVPT AES-192 #22 (P=0, N=13, A=32, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"6a798d7c5e1a72b43e20ad5c7b08567b12ab744b61c070e2":"71b7fc33":"8739b4bea1a099fe547499cbc6":"f6107696edb332b2ea059d8860fee26be42e5e12e1a4f79a8d0eafce1b2278a7":4:"FAIL"

CCM auth decrypt tag NIST DVPT AES-192 #23 (P=0, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"f9fdca4ac64fe7f014de0f43039c757194d544ce5d15eed4":"d07ccf9fdc3d33aa94cda3d230da707c":"5a8aa485c316e9403aff859fbb":"a16a2e741f1cd9717285b6d882c1fc53655e9773761ad697a7ee6410184c7982":16:""

CCM auth decrypt tag NIST DVPT AES-192 #24 (P=0, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"f9fdca4ac64fe7f014de0f43039c757194d544ce5d15eed4":"65fe32b649dc328c9f531584897e85b3":"8739b4bea1a099fe547499cbc6":"f6107696edb332b2ea059d8860fee26be42e5e12e1a4f79a8d0eafce1b2278a7":16:"FAIL"

CCM
auth decrypt tag NIST DVPT AES-192 #25 (P=24, N=7, A=32, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"f9fdca4ac64fe7f014de0f43039c757194d544ce5d15eed4":"9f6ca4af9b159148c889a6584d1183ea26e2614874b0504575dea8d1":"5a8aa485c316e9":"3796cf51b8726652a4204733b8fbb047cf00fb91a9837e22ec22b1a268f88e2c":4:"a265480ca88d5f536db0dc6abc40faf0d05be7a966977768"

CCM auth decrypt tag NIST DVPT AES-192 #26 (P=24, N=7, A=32, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"f9fdca4ac64fe7f014de0f43039c757194d544ce5d15eed4":"84d8212e9cfc2121252baa3b065b1edcf50497b9594db1ebd7965825":"fdd2d6f503c915":"5b92394f21ddc3ad49d9b0881b829a5935cb3a4d23e292a62fb66b5e7ab7020e":4:"FAIL"

CCM auth decrypt tag NIST DVPT AES-192

#27 (P=24, N=7, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"a7aa635ea51b0bb20a092bd5573e728ccd4b3e8cdd2ab33d":"6aab64c4787599d8f213446beadb16e08dba60e97f56dbd14d1d980d6fe0fb44b421992662b97975":"5a8aa485c316e9":"3796cf51b8726652a4204733b8fbb047cf00fb91a9837e22ec22b1a268f88e2c":16:"a265480ca88d5f536db0dc6abc40faf0d05be7a966977768"

CCM auth decrypt tag NIST DVPT AES-192 #28 (P=24, N=7, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"a7aa635ea51b0bb20a092bd5573e728ccd4b3e8cdd2ab33d":"4980b2ee49b1aaf393175f5ab9bae95ec7904557dfa206603c51d36c826f01384100886198a7f6a3":"fdd2d6f503c915":"5b92394f21ddc3ad49d9b0881b829a5935cb3a4d23e292a62fb66b5e7ab7020e":16:"FAIL"

CCM auth decrypt tag NIST DVPT AES-192 #29 (P=24, N=13, A=32, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"a7aa635ea51b0bb20a092bd5573e728ccd4b3e8cdd2ab33d":"16e543d0e20615ff0df15acd9927ddfe40668a54bb854cccc25e9fce":"5a8aa485c316e9403aff859fbb":"a16a2e741f1cd9717285b6d882c1fc53655e9773761ad697a7ee6410184c7982":4:"8739b4bea1a099fe547499cbc6d1b13d849b8084c9b6acc5"

CCM
auth decrypt tag NIST DVPT AES-192 #30 (P=24, N=13, A=32, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"a7aa635ea51b0bb20a092bd5573e728ccd4b3e8cdd2ab33d":"df35b109caf690656ae278bbd8f8bba687a2ce11b105dae98ecedb3e":"0812757ad0cc4d17c4cfe7a642":"ec6c44a7e94e51a3ca6dee229098391575ec7213c85267fbf7492fdbeee61b10":4:"FAIL"

CCM auth decrypt tag NIST DVPT AES-192 #31 (P=24, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"26511fb51fcfa75cb4b44da75a6e5a0eb8d9c8f3b906f886":"c5b0b2ef17498c5570eb335df4588032958ba3d69bf6f3178464a6f7fa2b76744e8e8d95691cecb8":"5a8aa485c316e9403aff859fbb":"a16a2e741f1cd9717285b6d882c1fc53655e9773761ad697a7ee6410184c7982":16:"8739b4bea1a099fe547499cbc6d1b13d849b8084c9b6acc5"

CCM auth decrypt tag NIST DVPT AES-192 #32 (P=24, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"26511fb51fcfa75cb4b44da75a6e5a0eb8d9c8f3b906f886":"d1f0518929f4ae2f0543de2a7dfe4bb0110bb3057e524a1c06bd6dc2e6bcc3436cffb969ae900388":"0812757ad0cc4d17c4cfe7a642":"ec6c44a7e94e51a3ca6dee229098391575ec7213c85267fbf7492fdbeee61b10":16:"FAIL"

CCM
auth decrypt tag NIST DVPT AES-256 #1 (P=0, N=7, A=0, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"eda32f751456e33195f1f499cf2dc7c97ea127b6d488f211ccc5126fbb24afa6":"469c90bb":"a544218dadd3c1":"":4:""

CCM auth decrypt tag NIST DVPT AES-256 #2 (P=0, N=7, A=0, T=4)
depends_on:MBEDTLS_AES_C

mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"eda32f751456e33195f1f499cf2dc7c97ea127b6d488f2
11ccc5126fbb24afa6":"46a908ed":"d3d5424e20fbec":"":4:"FAIL"

CCM auth decrypt tag NIST DVPT AES-256 #3 (P=0, N=7, A=0, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"e1b8a927a95efe94656677b692662000278b441c79e87
9dd5c0ddc758bdc9ee8":"8207eb14d33855a52acceed17dbcbf6e":"a544218dadd3c1":"":16:""

CCM
auth decrypt tag NIST DVPT AES-256 #4 (P=0, N=7, A=0, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"e1b8a927a95efe94656677b692662000278b441c79e87
9dd5c0ddc758bdc9ee8":"60f8e127cb4d30db6df0622158cd931d":"d3d5424e20fbec":"":16:"FAIL"

CCM auth decrypt tag NIST DVPT AES-256 #5 (P=0, N=13, A=0, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"e1b8a927a95efe94656677b692662000278b441c79e87
9dd5c0ddc758bdc9ee8":"8a19a133":"a544218dadd3c10583db49cf39":"":4:""

CCM auth decrypt tag NIST DVPT AES-256 #6 (P=0, N=13, A=0, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"e1b8a927a95efe94656677b692662000278b441c79e87
9dd5c0ddc758bdc9ee8":"2e317f1b":"3c0e2815d37d844f7ac240ba9d":"":4:"FAIL"

CCM auth decrypt tag NIST DVPT AES-256 #7 (P=0, N=13, A=0, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"af063639e66c284083c5cf72b70d8bc277f5978e80d932
2d99f2fdc718cda569":"97e1a8dd4259ccd2e431e057b0397fcf":"a544218dadd3c10583db49cf39":"":16:""

CCM
auth decrypt tag NIST DVPT AES-256 #8 (P=0, N=13, A=0, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"af063639e66c284083c5cf72b70d8bc277f5978e80d932
2d99f2fdc718cda569":"5a9596c511ea6a8671adefc4f2157d8b":"3c0e2815d37d844f7ac240ba9d":"":16:"FAIL"

CCM auth decrypt tag NIST DVPT AES-256 #9 (P=24, N=7, A=0, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"af063639e66c284083c5cf72b70d8bc277f5978e80d932
2d99f2fdc718cda569":"64a1341679972dc5869fcf69b19d5c5ea50aa0b5e985f5b722aa8d59":"a544218dadd3c1":"":4
:"d3d5424e20fbec43ae495353ed830271515ab104f8860c98"

CCM auth decrypt tag NIST DVPT AES-256 #10 (P=24, N=7, A=0, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"af063639e66c284083c5cf72b70d8bc277f5978e80d932
2d99f2fdc718cda569":"c5b7f802bffc498c1626e3774f1d9f94045dfd8e1a10a20277d00a75":"bfcda8b5a2d0d2":"":4:
"FAIL"

CCM

auth decrypt tag NIST DVPT AES-256 #11 (P=24, N=7, A=0, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"f7079dfa3b5c7b056347d7e437bcded683abd6e2c9e069d333284082cbb5d453":"bc51c3925a960e7732533e4ef3a4f69ee6826de952bcb0fd374f3bb6db8377ebfc79674858c4f305":"a544218dadd3c1":"":16:"d3d5424e20fbec43ae495353ed830271515ab104f8860c98"

CCM auth decrypt tag NIST DVPT AES-256 #12 (P=24, N=7, A=0, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"f7079dfa3b5c7b056347d7e437bcded683abd6e2c9e069d333284082cbb5d453":"afa1fa8e8a70e26b02161150556d604101fdf423f332c3363275f2a4907d51b734fe7238cebbd48f":"bfcda8b5a2d0d2":"":16:"FAIL"

CCM auth decrypt tag NIST DVPT AES-256 #13 (P=24, N=13, A=0, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"f7079dfa3b5c7b056347d7e437bcded683abd6e2c9e069d333284082cbb5d453":"63e00d30e4b08fd2a1cc8d70fab327b2368e77a93be4f4123d14fb3f":"a544218dadd3c10583db49cf39":"":4:"3c0e2815d37d844f7ac240ba9d6e3a0b2a86f706e885959e"

CCM
auth decrypt tag NIST DVPT AES-256 #14 (P=24, N=13, A=0, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"f7079dfa3b5c7b056347d7e437bcded683abd6e2c9e069d333284082cbb5d453":"bb5425b3869b76856ec58e39886fb6f6f2ac13fe44cb132d8d0c0099":"894dcaa61008eb8fb052c60d41":"":4:"FAIL"

CCM auth decrypt tag NIST DVPT AES-256 #15 (P=24, N=13, A=0, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"1b0e8df63c57f05d9ac457575ea764524b8610ae5164e6215f426f5a7ae6ede4":"f0050ad16392021a3f40207bed3521fb1e9f808f49830c423a578d179902f912f9ea1afbce1120b3":"a544218dadd3c10583db49cf39":"":16:"3c0e2815d37d844f7ac240ba9d6e3a0b2a86f706e885959e"

CCM auth decrypt tag NIST DVPT AES-256 #16 (P=24, N=13, A=0, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"1b0e8df63c57f05d9ac457575ea764524b8610ae5164e6215f426f5a7ae6ede4":"c408190d0fbf5034f83b24a8ed9657331a7ce141de4fae769084607b83bd06e6442eac8dacf583cc":"894dcaa61008eb8fb052c60d41":"":16:"FAIL"

CCM
auth decrypt tag NIST DVPT AES-256 #17 (P=0, N=7, A=32, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"1b0e8df63c57f05d9ac457575ea764524b8610ae5164e6215f426f5a7ae6ede4":"92d00fbe":"a544218dadd3c1":"d3d5424e20fbec43ae495353ed830271515ab104f8860c988d15b6d36c038eab":4:""

CCM auth decrypt tag NIST DVPT AES-256 #18 (P=0, N=7, A=32, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"1b0e8df63c57f05d9ac457575ea764524b8610ae5164e6215f426f5a7ae6ede4":"9143e5c4":"78c46e3249ca28":"232e957c65ffa11988e830d4617d500f1c4a35c1221f396c41

ab214f074ca2dc":4:"FAIL"

CCM auth decrypt tag NIST DVPT AES-256 #19 (P=0, N=7, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"a4bc10b1a62c96d459fbaf3a5aa3face7313bb9e1253e6
96f96a7a8e36801088":"93af11a08379eb37a16aa2837f09d69d":"a544218dadd3c1":"d3d5424e20fbec43ae495353ed
830271515ab104f8860c988d15b6d36c038eab":16:""

CCM
auth decrypt tag NIST DVPT AES-256 #20 (P=0, N=7, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"a4bc10b1a62c96d459fbaf3a5aa3face7313bb9e1253e6
96f96a7a8e36801088":"d19b0c14ec686a7961ca7c386d125a65":"78c46e3249ca28":"232e957c65ffa11988e830d461
7d500f1c4a35c1221f396c41ab214f074ca2dc":16:"FAIL"

CCM auth decrypt tag NIST DVPT AES-256 #21 (P=0, N=13, A=32, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"a4bc10b1a62c96d459fbaf3a5aa3face7313bb9e1253e6
96f96a7a8e36801088":"866d4227":"a544218dadd3c10583db49cf39":"3c0e2815d37d844f7ac240ba9d6e3a0b2a86f7
06e885959e09a1005e024f6907":4:""

CCM auth decrypt tag NIST DVPT AES-256 #22 (P=0, N=13, A=32, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"a4bc10b1a62c96d459fbaf3a5aa3face7313bb9e1253e6
96f96a7a8e36801088":"94cb1127":"e8de970f6ee8e80ede933581b5":"89f8b068d34f56bc49d839d8e47b347e6dae73
7b903b278632447e6c0485d26a":4:"FAIL"

CCM auth decrypt tag
NIST DVPT AES-256 #23 (P=0, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"8c5cf3457ff22228c39c051c4e05ed4093657eb303f859
a9d4b0f8be0127d88a":"867b0d87cf6e0f718200a97b4f6d5ad5":"a544218dadd3c10583db49cf39":"3c0e2815d37d84
4f7ac240ba9d6e3a0b2a86f706e885959e09a1005e024f6907":16:""

CCM auth decrypt tag NIST DVPT AES-256 #24 (P=0, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"8c5cf3457ff22228c39c051c4e05ed4093657eb303f859
a9d4b0f8be0127d88a":"677a040d46ee3f2b7838273bdad14f16":"e8de970f6ee8e80ede933581b5":"89f8b068d34f56
bc49d839d8e47b347e6dae737b903b278632447e6c0485d26a":16:"FAIL"

CCM auth decrypt tag NIST DVPT AES-256 #25 (P=24, N=7, A=32, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"8c5cf3457ff22228c39c051c4e05ed4093657eb303f859
a9d4b0f8be0127d88a":"c2fe12658139f5d0dd22cadf2e901695b579302a72fc56083ebc7720":"a544218dadd3c1":"d3
d5424e20fbec43ae495353ed830271515ab104f8860c988d15b6d36c038eab":4:"78c46e3249ca28e1ef0531d80fd37c1
24d9aecb7be6668e3"

CCM

auth decrypt tag NIST DVPT AES-256 #26 (P=24, N=7, A=32, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"8c5cf3457ff22228c39c051c4e05ed4093657eb303f859a9d4b0f8be0127d88a":"94748ba81229e53c38583a8564b23ebbafc6f6efdf4c2a81c44db2c9":"6ba004fd176791":"5a053b2a1bb87e85d56527bfcdcd3ecafb991bb10e4c862bb0751c700a29f54b":4:"FAIL"

CCM auth decrypt tag NIST DVPT AES-256 #27 (P=24, N=7, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"705334e30f53dd2f92d190d2c1437c8772f940c55aa35e562214ed45bd458ffe":"3341168eb8c48468c414347fb08f71d2086f7c2d1bd581ce1ac68bd42f5ec7fa7e068cc0ecd79c2a":"a544218dadd3c1":"d3d5424e20fbec43ae495353ed830271515ab104f8860c988d15b6d36c038eab":16:"78c46e3249ca28e1ef0531d80fd37c124d9aecb7be6668e3"

CCM auth decrypt tag NIST DVPT AES-256 #28 (P=24, N=7, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"705334e30f53dd2f92d190d2c1437c8772f940c55aa35e562214ed45bd458ffe":"d543acda712b898cbb27b8f598b2e4438ce587a836e2785147c3338a2400809e739b63ba8227d2f9":"6ba004fd176791":"5a053b2a1bb87e85d56527bfcdcd3ecafb991bb10e4c862bb0751c700a29f54b":16:"FAIL"

CCM
auth decrypt tag NIST DVPT AES-256 #29 (P=24, N=13, A=32, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"705334e30f53dd2f92d190d2c1437c8772f940c55aa35e562214ed45bd458ffe":"c0ea400b599561e7905b99262b4565d5c3dc49fad84d7c69ef891339":"a544218dadd3c10583db49cf39":"3c0e2815d37d844f7ac240ba9d6e3a0b2a86f706e885959e09a1005e024f6907":4:"e8de970f6ee8e80ede933581b5bcf4d837e2b72baa8b00c3"

CCM auth decrypt tag NIST DVPT AES-256 #30 (P=24, N=13, A=32, T=4)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"705334e30f53dd2f92d190d2c1437c8772f940c55aa35e562214ed45bd458ffe":"60871e03ea0eb968536c99f926ea24ef43d41272ad9fb7f63d488623":"8fa501c5dd9ac9b868144c9fa5":"5bb40e3bb72b4509324a7edc852f72535f1f6283156e63f6959ffaf39dcde800":4:"FAIL"

CCM
auth decrypt tag NIST DVPT AES-256 #31 (P=24, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"314a202f836f9f257e22d8c11757832ae5131d357a72df88f3eff0ffcee0da4e":"8d34cdca37ce77be68f65baf3382e31efa693e63f914a781367f30f2eaad8c063ca50795acd90203":"a544218dadd3c10583db49cf39":"3c0e2815d37d844f7ac240ba9d6e3a0b2a86f706e885959e09a1005e024f6907":16:"e8de970f6ee8e80ede933581b5bcf4d837e2b72baa8b00c3"

CCM auth decrypt tag NIST DVPT AES-256 #32 (P=24, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C
mbedtls_ccm_auth_decrypt:MBEDTLS_CIPHER_ID_AES:"314a202f836f9f257e22d8c11757832ae5131d357a72df88f3eff0ffcee0da4e":"516c0095cc3d85fd55e48da17c592e0c7014b9daafb82bdc4b41096dfdbe9cc1ab610f8f3e038d16":"8fa501c5dd9ac9b868144c9fa5":"5bb40e3bb72b4509324a7edc852f72535f1f6283156e63f6959ffaf39dcde800":16:"FAIL"

CCM-Camellia encrypt and tag RFC 5528 #1
depends_on:MBEDTLS_CAMELLIA_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"C0C1C2C3C4C5C6C7C8C9CACBCCCD
CECF":"08090A0B0C0D0E0F101112131415161718191A1B1C1D1E":"00000003020100A0A1A2A3A4A5":"000
1020304050607":"BA737185E719310492F38A5F1251DA55FAFBC949848A0DFCAECE746B3DB9AD"

CCM-Camellia
encrypt and tag RFC 5528 #2
depends_on:MBEDTLS_CAMELLIA_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"C0C1C2C3C4C5C6C7C8C9CACBCCCD
CECF":"08090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F":"00000004030201A0A1A2A3A4A5":"0
001020304050607":"5D2564BF8EAFE1D99526EC016D1BF0424CFBD2CD62848F3360B2295DF24283E8"

CCM-Camellia encrypt and tag RFC 5528 #3
depends_on:MBEDTLS_CAMELLIA_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"C0C1C2C3C4C5C6C7C8C9CACBCCCD
CECF":"08090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F20":"00000005040302A0A1A2A3A4A5":
"0001020304050607":"81F663D6C7787817F9203608B982AD15DC2BBD87D756F79204F551D6682F23AA46"

CCM-Camellia encrypt and tag RFC 5528 #4
depends_on:MBEDTLS_CAMELLIA_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"C0C1C2C3C4C5C6C7C8C9CACBCCCD
CECF":"0C0D0E0F101112131415161718191A1B1C1D1E":"00000006050403A0A1A2A3A4A5":"000102030405
060708090A0B":"CAEF1E827211B08F7BD90F08C77288C070A4A08B3A933A63E497A0"

CCM-Camellia
encrypt and tag RFC 5528 #5
depends_on:MBEDTLS_CAMELLIA_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"C0C1C2C3C4C5C6C7C8C9CACBCCCD
CECF":"0C0D0E0F101112131415161718191A1B1C1D1E1F":"00000007060504A0A1A2A3A4A5":"0001020304
05060708090A0B":"2AD3BAD94FC52E92BE438E827C1023B96A8A77258FA17BA7F331DB09"

CCM-Camellia encrypt and tag RFC 5528 #6
depends_on:MBEDTLS_CAMELLIA_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"C0C1C2C3C4C5C6C7C8C9CACBCCCD
CECF":"0C0D0E0F101112131415161718191A1B1C1D1E1F20":"00000008070605A0A1A2A3A4A5":"00010203
0405060708090A0B":"FEA5480BA53FA8D3C34422AACE4DE67FFA3BB73BABAB36A1EE4FE0FE28"

CCM-Camellia encrypt and tag RFC 5528 #7
depends_on:MBEDTLS_CAMELLIA_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"C0C1C2C3C4C5C6C7C8C9CACBCCCD
CECF":"08090A0B0C0D0E0F101112131415161718191A1B1C1D1E":"00000009080706A0A1A2A3A4A5":"000
1020304050607":"54532026E54C119A8D36D9EC6E1ED97416C8708C4B5C2CACAFA3BCCF7A4EBF9573"

CCM-Camellia
encrypt and tag RFC 5528 #8
depends_on:MBEDTLS_CAMELLIA_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"C0C1C2C3C4C5C6C7C8C9CACBCCCD

CECF":"08090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F":"0000000A090807A0A1A2A3A4A5":"0001020304050607":"8AD19B001A87D148F4D92BEF34525CCCE3A63C6512A6F5757388E4913EF14701F441"

CCM-Camellia encrypt and tag RFC 5528 #9
depends_on:MBEDTLS_CAMELLIA_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF":"08090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F20":"0000000B0A0908A0A1A2A3A4A5":"0001020304050607":"5DB08D62407E6E31D60F9CA2C60474219AC0BE50C0D4A5778794D6E230CD25C9FEBF87"

CCM-Camellia encrypt and tag RFC 5528 #10
depends_on:MBEDTLS_CAMELLIA_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF":"0C0D0E0F101112131415161718191A1B1C1D1E":"0000000C0B0A09A0A1A2A3A4A5":"0001020304050607080 90A0B":"DB118CCEC1B8761C877CD8963A67D6F3BBBC5CD09299EB11F312F23237"

CCM-Camellia
encrypt and tag RFC 5528 #11
depends_on:MBEDTLS_CAMELLIA_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF":"0C0D0E0F101112131415161718191A1B1C1D1E1F":"0000000D0C0B0AA0A1A2A3A4A5":"0001020304050607080 90A0B":"7CC83D8DC49103525B483DC5CA7EA9AB812B7056079DAFFADA16CCCF2C4E"

CCM-Camellia encrypt and tag RFC 5528 #12
depends_on:MBEDTLS_CAMELLIA_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF":"0C0D0E0F101112131415161718191A1B1C1D1E1F20":"0000000E0D0C0BA0A1A2A3A4A5":"0001020304050607080 90A0B":"2CD35B8820D23E7AA351B0E92FC79367238B2CC748CBB94C2947793D64AF75"

CCM-Camellia encrypt and tag RFC 5528 #13
depends_on:MBEDTLS_CAMELLIA_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"D75C2778078CA93D971F96FDE720F4CD":"C6B5F3E6CA2311AEF7472B203E735EA561ADB17D56C5A3":"00A970110E1927B160B6A31C1C":"6B7F464507FAE496":"A435D727348DDD22907F7EB8F5FDBB4D939DA6524DB4F64558C02D25B127EE"

CCM-Camellia
encrypt and tag RFC 5528 #14
depends_on:MBEDTLS_CAMELLIA_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"D75C2778078CA93D971F96FDE720F4CD":"01F6CE6764C574483BB02E6BBF1E0ABD26A22572B4D80EE7":"0083CD8CE0CB42B160B6A31C1C":"986605B43DF15DE7":"8AE052508FBECA932E346F05E0DC0DFBCF939EAFFA3E587C867D6E1C48703806"

CCM-Camellia encrypt and tag RFC 5528 #15
depends_on:MBEDTLS_CAMELLIA_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"D75C2778078CA93D971F96FDE720F4CD":"CDF1D8406FC2E9014953897005FBFB8BA57276F92404608E08":"005F54950B18F2B160B6A31C1C":"48F2E7E1A7671A51":"08B67EE21C8BF26E473E408599E9C0836D6AF0BB18DF55466CA80878A790476DE5"

CCM-Camellia encrypt and tag RFC 5528 #16
depends_on:MBEDTLS_CAMELLIA_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"D75C2778078CA93D971F96FDE720F4C
D":"B005DCFA0B59181426A961685A993D8C43185B":"00EC600863319AB160B6A31C1C":"DE97DF3B8CBD
6D8E5030DA4C":"63B78B4967B19EDBB733CD1114F64EB226089368C354828D950CC5"

CCM-Camellia
encrypt and tag RFC 5528 #17
depends_on:MBEDTLS_CAMELLIA_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"D75C2778078CA93D971F96FDE720F4C
D":"2E20211298105F129D5ED95B93F72D30B2FACCD7":"0060CFF1A31EA1B160B6A31C1C":"A5EE93E457
DF05466E782DCF":"0BC6BBE2A8B909F4629EE6DC148DA44410E18AF43147383276F66A9F"

CCM-Camellia encrypt and tag RFC 5528 #18
depends_on:MBEDTLS_CAMELLIA_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"D75C2778078CA93D971F96FDE720F4C
D":"2645941E75632D3491AF0FC0C9876C3BE4AA7468C9":"000F85CD995C97B160B6A31C1C":"24AA1BF9
A5CD876182A25074":"222AD632FA31D6AF970C345F7E77CA3BD0DC25B340A1A3D31F8D4B44B7"

CCM-Camellia encrypt and tag RFC 5528 #19
depends_on:MBEDTLS_CAMELLIA_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"D75C2778078CA93D971F96FDE720F4C
D":"070135A6437C9DB120CD61D8F6C39C3EA125FD95A0D23D":"00C29B2CAAC4CDB160B6A31C1C":"69
1946B9CA07BE87":"05B8E1B9C49CFD56CF130AA6251DC2ECC06CCC508FE697A0066D57C84BEC182768"

CCM-Camellia
encrypt and tag RFC 5528 #20
depends_on:MBEDTLS_CAMELLIA_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"D75C2778078CA93D971F96FDE720F4C
D":"C8C0880E6C636E20093DD6594217D2E18877DB264E71A5CC":"002C6B7595EE62B160B6A31C1C":"D0
C54ECB84627DC4":"54CEB968DEE23611575EC003DFAA1CD48849BDF5AE2EDB6B7FA775B150ED4383C5
A9"

CCM-Camellia encrypt and tag RFC 5528 #21
depends_on:MBEDTLS_CAMELLIA_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"D75C2778078CA93D971F96FDE720F4C
D":"F75DAA0710C4E64297794DC2B7D2A20757B1AA4E448002FFAB":"00C53CD4C2AA24B160B6A31C1C"
:"E285E0E4808CDA3D":"B1404546BF667210CA28E309B39BD6CA7E9FC8285FE698D43CD20A02E0BDCAE
D2010D3"

CCM-Camellia encrypt and tag RFC 5528 #22
depends_on:MBEDTLS_CAMELLIA_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"D75C2778078CA93D971F96FDE720F4C
D":"C238822FAC5F98FF929405B0AD127A4E41854E":"00BEE9267FBADCB160B6A31C1C":"6CAEF9941141
570D7C813405":"94C8959C11569A297831A721005857AB61B87A2DEA0936B6EB5F625F5D"

CCM-Camellia

encrypt and tag RFC 5528 #23
depends_on:MBEDTLS_CAMELLIA_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"D75C2778078CA93D971F96FDE720F4C
D":"4DBF3E774AD245E5D5891F9D1C32A0AE022C85D7":"00DFA8B1245007B160B6A31C1C":"36A52CF16
B19A2037AB7011E":"5869E3AAD2447C74E0FC05F9A4EA74577F4DE8CA8924764296AD04119CE7"

CCM-Camellia encrypt and tag RFC 5528 #24
depends_on:MBEDTLS_CAMELLIA_C
mbedtls_ccm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"D75C2778078CA93D971F96FDE720F4C
D":"9DC9EDAE2FF5DF8636E8C6DE0EED55F7867E33337D":"003B8FD8D3A937B160B6A31C1C":"A4D499F
78419728C19178B0C":"4B198156393B0F7796086AAFB454F8C3F034CCA966945F1FCEA7E11BEE6A2F"
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
   <Configuration>Release</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\pkey\dh_genprime.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">
   <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid>{718960D9-5DA6-7B56-39AD-637E81076C71}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>dh_genprime</RootNamespace>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>

```
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
/>
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <LinkIncremental>true</LinkIncremental>
```

```
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
     <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
 <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
```

```
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
   </Link>
   <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
   </ProjectReference>
  </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
   <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
   </Link>
  </ItemDefinitionGroup>
   <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
   <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
   <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
   </Link>
  </ItemDefinitionGroup>
```

<Import
Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
<ImportGroup Label="ExtensionTargets">
</ImportGroup>
</Project>
HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,0,0) #0
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"e91b63309e93d1d08e30e8d556906875f59747c468b0d0da":"":"":"
":"b7928f9503a417110788f9d0c2585f8aee6fb73b220a626b3ab9825b7a9facc79723d7e1ba9255e40e65c249b6082a
7bc5e3f129d3d8f69b04ed1183419d6c4f2a13b304d2c5743f41c8b0ee73225347"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,0,0) #1
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"d0c57f7dc0308115b1ea30e2ea2f770289cebdda617d132c":"":"":""
:"b797615a78d1afe74ebedb9d8948d82cf2bb586ed80146b96d41a709f689178b772dd342d29af5449694bf8eaf33a66
4a24c0ad29a12529eeaba478a799917ab4666de1b6eb2c7332017d67eea6fabd8"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,0,0) #2
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"286e9d9e39e4024dea0c885fd6f7f107586b6a1a8ac3ac0e":"":"":":
"ca25aa9ef286a3cd52d101db01cdf0ce14c7add124f1b6a9a8b3a48c74989baf01f6ff704da7c5d5785b6e9c219148921
02313e7a15cb2f9977a513ada0d3f242819aef2c1699b72cbd358c59435101f"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-1,128+64,0,0) #3
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"6b20dda65a96f564fc0253d38dbc290b813e538d040d8dd9":"":"":"
":"66b6ef57a3282838dea05d122ccdfa842dda19333ded2015d381394da38c8309a6e9703ec065335b116efb97daaac9
c53ceb7a218ed0db61c3ba969dc629b95f5418eadfa43c58714fb02176bc0b17ec"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,0,0) #4
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"32339fc82b655051042e3038e3161c4fb252e495ff396be2":"":"":":
"e95e4551a37e338faae4419e3a70e4c1e3d516be7e554cabb00007c591ba7cb6c3247889a9b08e46c6619f166d996e4e
34bbf6cd8a354de9964de906041f73f2ade2eb82c6e82627d3257738c2821fcb"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,0,0) #5
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"deaa9d0c2ca7a05cba12eeb7db24277e1605e1d030d76ddc":"":"":""
:"bab5be6001da5951c1e7873f4e2be318e879370eae8a51ed8424ed6f12b2d294b45d006b1c2cd8c1ce047fd16f2fbbc0
9954a8b464cc986f23e86e1d9398d20780190aa5be0505cdfc826c7a01dcab99"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-1,128+64,0,0) #6
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"589766be3c03b0a351a81b1203f944e2928e95f8a3bc7452":"":"":""
:"5bee2482667220462ac6d3c234f7333703c5abced2ff2ad91d52193e86a61cfa43be0b4f7e831e1e563e260178f23976
b2f3e132356ab54567b37580bf9d751223fad7793f0ac11fc450817536116b1f"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,0,0) #7
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"07cc4d22b010335045cca142d91494bf4d5e842af4155d17":"":"":"":"8e13a574d17dc8b44382d3b263e857f50816755917603a07ca4987fd40340042a1e6a82a227647130304d73d8704fd9ad4db3ae42daaa55b1f93948e70c451a12724fed870e02a1a8ec4eeab716c6854"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,0,0) #8
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"6425624a98ab3018eb4ef827f5a4fbbac1022d70155ef375":"":"":"":"16fd6abb10dba1659ed56d4296b65fe3f2449996bdb8eee5c94b249f04808cdd9563569a4152bd99a32592d35d6a4cc806c228284487fc1e088b178d4c8ecb6b0e3cfaacd7d39d754d8bd4e6662f44a4"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-1,128+64,0,0) #9
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"01d11d2b631be240de2f41d10bdce47c89fa32427410cc61":"":"":"":"4640a063e65ef0c0de97f98a39297219e2a1eceed7e6426199719911edbb3d06fbde6fbab83878e9ba9fa8e1d044f7a40f3627d7cfc49d17f101ee64f6b8c6e6154a01b4d39fb9ba6b33ca2c27f9fd52"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,0,0) #10
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"5e0a89b3aba1cf5ed94756083726de8db5d79162f73a5031":"":"":"":"cae7b2c25dce1c12e2c4f61b3e53155b9177e92bfb8faefc425d1cbb507713921378ed880986709bfbd7cda66d18dbe0732137a86d47b7e8223e345af0cd9a0219ba290040bc6ff44c1de5b16f32b933"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,0,0) #11
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"3b76d32d5982daf6e2164340941a1707441bbb99a2668ba4":"":"":"":"63640e406e16b3b82723a6cb3830657b756fe61cf2ada96f667e0f2df0c9d33c6f164ee78d4976281a84d3024ff67074acecd65391a84aafaec9d6b088bc33616543b61a4c603e5a21bd39e2a72401c8"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-1,128+64,0,0) #12
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"45fcafba2278bf8e6d437396f60f0e84654de44e0bd6cb8a":"":"":"":"7e2325cb2ced372b640c2496a3970cb7771fd494e40ae17239bfffd9ea2ab0ee74c2d3c369328a3b465e67bcbea86f50a32f9ff820505df5adbc032d3adb83581443877f85c60b3b701f59b1fc38c063"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,0,0) #13
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"4201db977ef90d08f017c8e38204c2995bbb47efe9fa4cad":"":"":"":"101c7318e26693bc11d64b780e9b32d4d958c7475ab99fdd6fe86554dcef54ccdc2ca9f4ec355eb25d7b3f570ff95ec7abc2e9e2fb879bb045debf6c8a98ff46668c0de21bd8d4d18fb9e11550878e32"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,0,0) #14
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"5d80883ce24feb3911fdeb8e730f95886a63c01478ecd62b":"":"":"":

"9e351b853091add2047e9ea2da07d41fa4ace03db3d4a43217e802352f1c97382ed7afee5cb2cf5848a93ce0a25a28cdc8e96ccdf14875cb9f845790800d542bac81d0be53376385baa5e7cbe2c3b469"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-1,128+64,0,128) #0
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"32c1ca125223de8de569697f92a37c6772d4cc4f0544d409":"":"9e98cc8e0f8eb84d1911c1775a5703bb":"593aa3a300e5c907a011dd5a3dcd77e2":"942909a9d380aa5d4e3af69093a8fa513ee545b9bf9e1b81c5f30966db3e5cb52f8b1b6fe440d592e5fe4a972c36aa498035e2442f82910c5cd095c7f4b4c7e7555c4669cca481cdfbfda167b5d6f8d5"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,0,128) #1
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"172a2d24ef128dadc93e0b74f277e7c3692f86e6ca5e1117":"":"93b4a1fdbf9dd30996298804dd86c0f7":"69d792dc9b6fe1601f31a68e4d007187":"13f30b4698d6e973556c3f92dff6241bbfbde300ed58d07fd5f64efdcd0c1b62ca3de6358d505dcf972fdce20f7b891c4cab493721d80cb108fcee915835b02dea33041b38e28252c30a71fad85878e6"

HMAC_DRBG NIST CAVS 14.3 No Reseed
(SHA-1,128+64,0,128) #2
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"4a17b8069ae3a74d77c9c94514ba90cd2abfac0002d2c5da":"":"cc39d1a2a425f00e220d721fbfd5b6e5":"1ccee25f5868e863a05b72d744e64aeb":"d787b355629779ff2916397d6094f44dec06337571ccb0abf5a17b6cfabe00557894e9ddab8caafef467faa4514582b5073e7d1d9fdd6fa34c565d1aca23742ed4e87133253a9664ec085bc6c76965f4"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,0,128) #3
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"d60c4860d9ba3ebb64e2095231e07792ba6b5e9e22e14043":"":"776273bb22f5e62a793692127bcbd785":"8795e45f82160cb1096a509fd3572f92":"3122c1d3a6de8b25fd180b159731f975f78601360155e43f694b289822a25948d2c20a673f181be06b59c566960339f25015d2acbf5c7d3f68a2bade779e00faa24623c1313da888dc8cee901fa05573"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,0,128) #4
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"494983c04581b811e0b2b846c54bd31824bd70fd182558f1":"":"935200a7edf1e2903581fedb7c04533d":"49c0133cca2457fa7cbbd4c68cc5e78f":"0fd2ec47fa2e31326ee9b894fdd6224818190168640d91a2a0c247b1e27ccfa343e9370d182d95b2b5bd74b4b09c44d04094364a6fd02ba70ee2c55e04d65ad9c6da65b9c0742f9fb5ca95daafa48df1"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-1,128+64,0,128) #5
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"77ea86ce59f2466e55ce2057e7855035c09295c02f1c51cb":"":"f36d65f22b5afd3f51e13ea38dcff555":"6b613b56e470b5c2c30c30aab9a772e1":"41cd8ef82609012d33b4e5b51a39ec17eda4317962627796f7845045920becd7caef56d4a2c3a8e849e299babe92367ef34a8910bebd498248ccc2b3f5f63920b31cfe856973e15e48b060871a9cf9a7"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,0,128) #6
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"2dffb03703023f65b757b7ee87899a14a9c8ce788fb2bddc":"":"da42b213071252adb755a6cb24094c17":"c83fc2beb60a7ee9b374f3fb7bfc8900":"8f54271e3578e60e8989e49f5b426e1a0296afbfcc7da0ffbdd5dea71ec6b339b6d866bd3756ba745e42c8cddf997cac5fed72b33ac81e5f4d6f2d15f030a41c684552fc94d48c0d97323ef7eb656857"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-1,128+64,0,128) #7
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"890e7323502313bc7d617805360d5968b6c68c0280cef5ed":"":"257f1f60cf2d36924c3e7b6e4cc35135":"89235cc472c6e2e1e92c70324459a9d3":"55283453e82662c8d92f54cb4a5d784e83b1b3527bc5e71a53f04508172eb5156ba2a9ba92116cdaceed17118c7637af4b574d364187a52cf0c20d768da518021c3d95cb5ce6bc108b1bef19bad66677"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,0,128) #8
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"167ce6bad165eb640eebfece7ca6690ec5c6b5f8c7fa9304":"":"c0e7ef13138ec4a7d52baf8592484ca0":"472a47e3fc098c7cb92fb953a26e25c6":"e2aa2650c84be79ec410ff9bac93e5caff8a46a8c39495856ff64c8c5399e81654ba90c8a8b26cdca2810ce68e4ab646e50a1f6fa7a829cfd72c9a61e1a0b415c031067dcd417baac9553cf7d84a7742"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,0,128) #9
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"6b8aeaf70460e83a124899d705dc0900acd811698669fcee":"":"94a53808df5ebaa7693934d7fda92b95":"4d4e7d88f44fe556c5ccdc56f8b2f098":"165aae6bcdd799fe325ddafce3b645900eabc87552c0bb47ee2eb6ad51462a8a4f4498c4bd24fcfc46de5d12351143d5a838060f617258c218035a4f29fb34a54673205b2e1b362991693d7b99972954"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-1,128+64,0,128) #10
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"00f30f92bd44a9b2b04a6cae67533ed85b4ae1335b98109a":"":"77ec4274fe5f8f22dbb4a1ed6050811e":"ef041b6516825d51bf76d2f651a55576":"8c664357b01425668ea5daf07a2b5b8c50dbbd71d9f48c50f275a02b6cfc4717eb7db286fa49f17d05d44230f7d82c251a6f0fe0a2add5d2cc9a92a527f63a9bd3c8ec93e9a404e0829629c5eeb997b0"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,0,128) #11
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"2eafeebb58a2fb54474280112c5668d61be2aa4df98598af":"":"389a36ecd687080a5d2cace8a326f03a":"495965bdbbb1bb01ba61191e9dd4b038":"f17db045b0af4913d79f99e018c1f726f4fe02f08477cccc0d6a068a808bfc6ccb797e6022dc3b99ea18086a56428884110c49128a51e10c15f6ecbfe0a5a1e97e72a578fefea6c66c436c91a2b6395b"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-1,128+64,0,128) #12
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"b6497197b783d1f493a6430748b45932895ea2a9d8204f5d":"":"ac

26665e796d1b00951c725da88d992f":"5f08c7951106dfec5096d90097449cc2":"170b58ac3342a968c96aa29f1ce820debe7934d9db46216c03ae3afd304188cd38b6208e1cad5fce5c26179a30a8771015a99d2902d51899ab0c42e0b400d18f1e89411248db96f9d62b466f828de150"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,0,128) #13
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"4ffafd1f20dd38699bfca029c0558483fbeed3cb29aa0eb8":"":"96abfcee883d8dcad967c071c12dde19":"9fd7cc292cd55d8364862f5fd675c08b":"5e8612c6ce8f5b6838a1e4fb9e14370fb2d66bc885f6fe8a3ff232f16340c2af58eb2734494e0ce920f36046b7a807f4b55caf3a45bdcaefa4bb23f352601c0769749f0257428918b931606c7b395135"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,0,128) #14
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"89a6f070afad5ccf4d117c4e44baa2c7b28941fa7e828c04":"":"7206a271499fb2ef9087fb8843b1ed64":"f14b17febd813294b3c4b22b7bae71b0":"49c35814f44b54bf13f0db52bd8a7651d060ddae0b6dde8edbeb003dbc30a7ffea1ea5b08ebe1d50b52410b972bec51fd174190671eecae201568b73deb0454194ef5c7b57b13320a0ac4dd60c04ae3b"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-1,128+64,128,0) #0
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"49058e6773ed2b7ab309c0949fdf9c9ea457cb8ec0e7fd01":"dc477641d89c7fc4a30f1430197dd159":"":"":"4e891f4e281100453b70788929ec743a3c5edd9b81dc798bc93771368c39b612037b6f42f60c5d8924b646848151b0c295be491d4a28d1927deed523fd04d3d2dda95ed42166312e5c3392d22893b0dc"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,128,0) #1
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"4ccc7d83009a28db14e839176774d45d9345358f336a1622":"e6db32976d9262b1d3dc487f22e1f5b3":"":"":"5a171e9f0065ece37ba53df81ac3d88054d53d0cb695a901e1a1ca91352420b508c461ac91095ccea81621b800ddcff905020f96dad2a50377d3945047420c3b902e8e361f4525c1d4bfa8af164925d2"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-1,128+64,128,0) #2
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"fc7d0c3ef1c404ada968dae35581b6cd31e0a46c39ce49dc":"14158a65fc9b3bc1ac04c7854493852d":"":"":"918494f47dadda22667dc1d066f44f3ccbb61d3f84b2eeab7d26f4e999aab94e79d282287ab76d4e3eeeef2ef79c2ad571382abdea55d5d8642f604f8f27f3f73a5bc1413dc87bfdf91da1c6045ec223"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,128,0) #3
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"1f0df7933dc99eaf7b284b02ee773ec46461fd762c595408":"abd1d8af4ae46d7e5f1f4e0b71b54edc":"":"":"f1eba7596c6c20118f86017ff86514d745ce7ea02c49719094e5c2a96d3dfa1dd5079b8eff8078ba9793900dba145a260e672837422c351c3f231c201dfaa21e48d3f7ee28bcd08dac680e80bf87ec20"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,128,0) #4
depends_on:MBEDTLS_SHA1_C

hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"09988a36abad74c3cf377db9c9200baf6c27be4e21932166":"17b7a40f4c37894bc948456e37ad482a":"":"":"091e5fb9c6c218f2460c514fa215061460ca90cfb35c1a9f5ea125fc49aa0b2beb42dcb0fed865f8510c3141cd51d1b33216e2e72cebcabd3e1bc0eab201d8e72a0d1de1c2b7915a0cf242708092f211"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-1,128+64,128,0) #5
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"ce1934b6561ebaaa851accf8ceae5b0dc587922ff68836aa":"602e9086f44d03ce61039c2e81fed620":"":"":"441da7552b2d45533fc924ea985fd4b0b95942fc7997a37128d3e96d4c2792b241dbe921d61f3898852d4f93740cc3649cb5279a7f0f09be3990e9ee599fb0717c308e7a939a441b5c3ba0cb8aa19647"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,128,0) #6
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"58f1a9eb935fd08a4c3c894a06ad00ca0576589700a4d50c":"b14f2a74cbe3881069f30507919c6870":"":"":"ae9c6b40d951aab9c2d9cb920a05f3e154898c83e392dfbd7ffcbe2283eb2b75842fa5e7bd9626ad12e814874f1966fea1eb817793d2eb0a9cb9270cc9aa4267118fba0c7b6fcf487a97ebcbadc67496"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,128,0) #7
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"0abf2f845295bb1dd283daa24e75fa08c9e9202793c479b3":"f8742f44932bae2d65a032ada2b76382":"":"":"8847696e8edd2c7b751b780a6fc69d8434a3144593936943217465362b3c3f7b25b75149f7c69d10ecd169f00ed98b53e0e498af6d9f600441ee2c01a9e74ed845d24cdab4543dff7d1f7800a278671d
"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-1,128+64,128,0) #8
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"0f9bc6935e7baf17d560931ec3e75d9fda7b19214e0ffb9c":"c13bb26e9349a56866f821c10a2ae28c":"":"":"12a849651f310fbae04c4da4680a21a50a9889806194be470b8b111a32ea741794cbe725d98ae9d40c0d60c04c8b7b32917f9dc18c27dfb8c64579a176a2c4b23cc32e5237fa5f904ab1249aafa7cd88"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,128,0) #9
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"79d96ff5ec92af9fee0af7effdc15ce56b9cbdfbbbe5b49a":"23d1288ae41e65e56e7b783f85ae8b47":"":"":"206c2564950995ac6ca6d2ad51e9cacd7540f254a335d6d7eed7ef17956949cb5d7d3f4e197e82aa4442d08d1d0f933e641f703be1be4a9ca5747e524687a7a034761493dcf2e1101789f135de5d3f49"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-1,128+64,128,0) #10
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"94e852ffbff4f20078181221b5fbb8048f3e95de313a52c1":"1841dcabae24c156a17a1d0eda6f8bb2":"":"":"15319b06c05d47deeaeab540e649cc6e2989843de07dcaa966d799a36902f72943585e2773912040185ac1efa060c6edecef800e3116c66ccfeeec9fe7ee70f3dae2ac1c0210310ea164f4c4402d2f77"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,128,0) #11
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"473c743205bb375fad15f537dfeb402d879754b2b4987cbd":"4f88f4db50a6806d6899f71981beec49":"":"":"46b0694bc8afc6d86dcb8b80cf8815104007ebedb06050ae625b890060c4da

d3d9e2661042d26a3cfded0383829ddcf616ec84d3f32d307480caf0f87ba9b00e88812f5cb2a4e94e354092d0c50b9bc7"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,128,0) #12
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"20208c9ac4830512786fce7ebde344a82cee0d7d7a5607d6":"2602c5f52c7ee2620486ce56366cc8eb":"":"":"b0bd2c0739ed1608848dd0e9c1db9f547c64268754af09716da40b2682fbc45f56de954cbce0d8a3f53eb2c3afac9e3afeab4038fe042c897786fd3da70f2d6b62b12981630bf30d76dd879e2926ab40"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-1,128+64,128,0) #13
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"3011c31a44ccfd1260ae9e431da41e883b1a6ac9060f2fa4":"6b36a1fcb2a2173fc7e0c120c2627a6f":"":"":"a781d9970c7272e98d941438d311cf7e80d2d56b29eb0b4b1c76d00908401ec5b4bb1c5f159dbf42ab30100933b1628faa92d2e25bd37ead4c3354c823013cd9e331bdf5e2c5c7d11d5bd9f50fd110fc"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,128,0) #14
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"ee6d57635e5ab4b3d73a2652c1443b32296bfe331b6578e6":"4fccbf2d3c73a8e1e92273a33e648eaa":"":"":"90dc6e1532022a9fe2161604fc79536b4afd9af06ab8adbb77f7490b355d0db3368d102d723a0d0f70d10475f9e99771fb774f7ad0ba7b5fe22a50bfda89e0215a014dc1f1605939590aa783360eb52e"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,128,128)
#0
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"c27f80b1d085dd15cb163f0336d077457ecb3f32a90242f7":"4deb622a31b4c530348b5f08008fb7ee":"5a84f94804e2d04ead773d2a324b34d6":"226d9f4d720f580c2be44d4eaf2ec8db":"6db76a0a003a64dec6801dd3271fae8a43aa8ce2e0d205e3830e267072abe28d2a6f707494d15638559fa4282843760daa90eec5d2865ea11e836e60345160d5112445ab1754b578b55471a1d9caf275"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,128,128) #1
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"517dadbd6e20fd83aeaced197732b1d5ce221a60f8210685":"bd9911bc192da45c00c47d5ee079473d":"33254154ffeb4983d27ac08980ec4943":"349db52f09422883536d11ac4aaaf7ba":"dd7be811d3a9fdd194e8f8f18b35e1d9f1788844c371d811cb898ebc561d000cc285afc8f486dabe37d6c85e614d3d196c544ca560ac6e0337b0700e1ded8fb28903e66329afdd589308d56c50d73803"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,128,128) #2
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"c763149ba95e7d054da52e4d3d06287253bc2f43ae7c9da0":"305d6aa3c6148a0eb2e91b9385de5903":"a36918edaf5add6f0f81d3f991ee30a1":"5c65b09e744317db86d78aaefa66af44":"5560d27fc55b885a29a449a1f8835966549c4956ebb0393ba9fe748e74a5a303f1478bb3e507a9daa1159dd8dd6d171bff2e3830581d7f6fdbccd91a8748d20c1d981cf909c31db6eedf5587722ac257"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-1,128+64,128,128) #3
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"b479a14d125fe4601053989439f85200e198df756aff7543":"8f5906

70f88d8c2c713d63643f93ba55":"cda7c7ee77e667b96ef0ba330c9ca6ac":"a60fd147f6cdfb408d160e388c20d8d8":"5f088bcebd816551c4b22c3024aeab2f75c906dc8fd0ab0c80055e0445c1dc151a06df81bd39b8535261a7a5dcedc7f9b17c062ee6f120f2099f2ab5aa93f27a08d7b5cf1027e26adf54a520916c2cb4"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,128,128) #4
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"bd46fc253e9334d4aa8bdff5e21c12e261515159b01a4516":"1735486e5ea8be74fa158b2fea8e5cad":"c3517d58cdbd0262655174cc1d1eb324":"404f7b8eb461d077368e2ff06ddb4189":"7f1cf172b67ec7c566c9e24c071b79b5a4a135a369ded5e78b8cd2467749e30c401bf176d88cc0e05a587bb2b8ed09206bb314df59009e88a01ef007e61eba2e40093aa003dada48314869c0f3b99d50"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-1,128+64,128,128) #5
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"600a31b8f55c85ce27ece4705e6fe8cd17a01e7827ec2383":"6deef06a079ad2062e77dba21fef6441":"ca5512ab329ee941b22f327fe0dad499":"c1ffc97289d8d363729daa1628a2c735":"a81cf5563940ffbbee9dbdcaf7db1e7e53b427fd3a0e795c35a1b8eb6f6316e43b804690a44897e0f42fbdfa8c9f1777024d2a530eda994ed038de60b90602545cef99b69f371f79619babda9360c665"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,128,128) #6
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"f38b0cd16e9434da916b63e8b7ce1a91883ec208c3baf76d":"534799e3fe51bc370af6568072e2e579":"9520ad24a61d29716342d2b7bd35dd45":"c4e92d6da37a9f6236a396f352c53c86":"5dc0b3bebde5bac6d4d24ec08f1510dc88e1e06c97c3031dc9519f3392e83a09e1a7db99b2148d992a928bb5c1f68265086f7a84e697a7a0aeda4b41590606ed139063def46fa2a625657b17f18845cb"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-1,128+64,128,128) #7
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"06a5e76d0ee90ed0206a07a914dc20796a8a2fb2c0ebbf14":"2a49312af91926a37b5f7c009e8047ef":"0cda72090ebb007ab27156957e64e7bf":"24695b221f42a5be6d4399c6444c4aa3":"2b0aeca45ed44ca34a2fc741c5e4e2091e115a4148e71bd8fa90588e32253ffcf360df213b48a19f6f45186b67dcef6327729ac8f3c08d658de89e71539783fb66ae834455407e7827114317299835bb"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,128,128) #8
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"6c12df5d2ba1f6a6e1e733baae42daafeb47cc188d1b0be0":"f510139561b292a7a1a0292b7de4b162":"f57a0c1dc69eae7473394ad1b950dc61":"9dded4779fab0c8843fa693146837689":"2be15d2ea87099a8c0430ba8e9451208a898379da075169568196f656eadbab59637c1f949b4506a851ae0394e135542137bd0daf1c188decfce92f6ef2396aa5bb125cf3187230ac81c3864632d9234"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,128,128) #9
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"0e6a7843e29e5f16d2bbb4021d6389ae692298b9f62ad22d":"f0434f112699d116cfa7eddad486c544":"146eb042377cdf6a0831558ac17ad971":"b29c26d483fde8489263accafc10d698":"ecf0812aebee7a452339071d9906709fe00fccbb0d94cc101b507646f554ebf3602459a4f20b82325b0e083ca189f59d68c5753dbe942643f07c7afcde99f9d0cc2883923cb80456fcedc535bfa7d647"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-1,128+64,128,128) #10
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"b6bc57d663b671868265fdb756e142fe6da9c07dd0821c6e":"f43c5223bfe726a3164afdcabe931eb7":"ddf419d8e074a4ff2daf06a1adad4bed":"e0862e71c4ac52194cd320d196e446a2":"4f9b9e9aab493571160c732881dc358f73a08450a152124775e559889a9298d034ce1882dd2116f4863f1524393e1a3f1aceadcd9c4163dab7c543cd375c3f4b61ed72475d1812017ac83bf22846d14c"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,128,128) #11
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"f5649fc184f33c63cf8484011fa27578c1651fcd1a0780c6":"153f7b2c9bc9494a20ed0bf16b97ffdc":"6106fd4fe0e1d894837ba8624cebbe2f":"fdc2988e6b358929645d27594fa98df8":"49130a750b4758e7e8dec8d82bf66ae771d51181c33cbba9d84093ee4f83f6e3aadd3f40fbcc441fcf90ed83b83c9d9671b9092907a36231ec3e2c56775c5699fce16abad104b291dd13f67ad4e1ff4d"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-1,128+64,128,128) #12
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"fc3dfb2f29b649391437aff6920760671e470ebf09e8fd68":"4e7d48fe49ecefebed749979b965d8f6":"ae7405de4957947dc09fb1be2227c763":"3fa22158d9bb1948c64102f3ac00bfed":"ffb49be8c714b502595da9248248fb009eace24ff77d298dfe8b05efe6441352213bd236bdf4b3de34fee35b051747f4e549f69bbad8c729f3b5cf2db29a0ab6aeb590857e0f48babff3a9ea3e4079b6"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-1,128+64,128,128) #13
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"32018afb07a6141e9a6badda9b647f650090ba3475d0149b":"fa92f66bb7a06a1652d4084c15d2f778":"13c32c456c799cf0808e00c6de7efce0":"693728213798dde84176dabfb50434d5":"12c9d6683e6ebb5136253db60b39b3203f52607e44d13ae80709cdf2fa61ff5befb0838f544e39e135830b573ac5a31b7535c0a2502370400906658e6b1e9a0f5755f360d9bff68fa55ad628b49a8937"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-1,128+64,128,128) #14
depends_on:MBEDTLS_SHA1_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA1:"3e325daab3301856044f416f250b6161e447e63d85ca084f":"a9d2a53dbd7ef4b9150dd0ed4d002e56":"4de6c923346d7adc16bbe89b9a184a79":"9e9e3412635aec6fcfb9d00da0c49fb3":"48ac8646b334e7434e5f73d60a8f6741e472baabe525257b78151c20872f331c169abe25faf800991f3d0a45c65e71261be0c8e14a1a8a6df9c6a80834a4f2237e23abd750f845ccbb4a46250ab1bb63"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-224,192+96,0,0) #0
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"a76e77a969ab92645181f0157802523746c34bf321867641051ed6ba39368033adc93d4e":"":"":"":"8925987db5566e60520f09bdddab488292bed92cd385e5b6fc223e1919640b4e34e34575033e56c0a8f608be21d3d221c67d39abec98d81312f3a2653d55ffbf44c337c82bed314c211be23ec394399ba351c4687dce649e7c2a1ba7b0b5dab125671b1bcf9008da65cad612d95ddc92"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-224,192+96,0,0) #1
depends_on:MBEDTLS_SHA256_C

hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"65cdaa5ab147d0c79fdd02b24fc94d0e427f59ef9a31f447458c6b
efe0c2cde5a58c6b7d":"":"":"":"0d164682b5bb552a53a2a942373639d98576450ca632faebc15060691a4219467c5aa
106034cd19a214a0a4f31d402e68c4c565f49b33b680d522ef25f541e8202be779730376fdcf5b7b58fd6ac959204a88f
91008651d2c02ada82505f914d4d9b9aea7967784e5320e185e1248270"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-224,192+96,0,0) #2
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"650996f1477112af7604386be5ace78232904315d99d87d72a067
09d331a6f930b447cf5":"":"":"":"d3341d7767cfd95640a107b3abaed7b4e1855b348e3ae5bcc53a0b0d49d4b4976837
ec8f376f38327135578eca7ee583215bd5c79ebf499816f79afcc402ff1e9ffc4ad0f896761c9cff75050bf84baa194c3557
63b16b5d2648d480a2b48f22662685de39c7cee90aa0b6edf8062e42"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-224,192+96,0,0) #3
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"898640ce467201a53e7731bdfb572977f7eb3e49050bc1e367ca7
4bf0a27376d339d09f4":"":"":"":"4f5eea927023b4abab5d4d9944e84ca001ee081cbc21d4080e1534ee6d1d8a6f60361
029ffa983bcc79b5d65d4aaaaaf98983de13ddde39a739f9d95878fb31f57f96184e5f2f3adf654a468c616237fcbc6b2c1
94e247178cb90294f631c449a01f1fe09c02587c460305be9fc71b5a"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-224,192+96,0,0) #4
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"fe405dd73956bf6ec875515eebd8c5ecd60553643da750914c83df
c93611d57390af7324":"":"":"":"d8ae0eb81913a190c439f8ffa56c06155a73f84b20608b2b2e9eab3061202cebad18ab
8b3eba81672152c1c02ef573cd6e8623c392facb6a857425c6795cd7999c1e7f56f3fa9accca018076e0bfc106d075df98
f5fb66f28933215e9276777dfc479e71a8d506a66197918d9b0f7a8f"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-224,192+96,0,0) #5
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"b06892f6f455afddc8eb60aae35b35a64f63b2aa85a2dae4ef48926
6f7bc354f72d68b71":"":"":"":"fc10c03fc37d3bd5fba6591a97f6354a9ed8ba2b6806744432851f43a3ce6418e39ccb4
17b8539e349acea588e2abe5da06147c9825c6e50a31f8589a57ca3bfb10f0da9c8e89fe2e372b5af1cf96e0fbeec5d992
28770c41a76e587da7d8764d5f235f5d1d6188d84ae61c52c2164fb"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-224,192+96,0,0) #6
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"9174e174e9e031f62b2e19ae5c0bef22eed7d5598e6e73504759a2
c15b05c2473a721d26":"":"":"":"1962f2d473b31a2576dbd78022f4eeb974641fa2e9cb582f03ab741929f51f0f466312
9e68ddc242e1c2ceafacec3dccb97e09527aff46b948f0abcea1451699dc3ae4d3fb5e04c84337e17b504af2fb5f1aa6ec0
033ddf138a188ee162c497526563a67da8015275d89f0e1e902b2ef"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-224,192+96,0,0) #7
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"eb1d45ba0d8951b7b1d7ce922b7d1f6e94da8b821940126c9da5b
0b4382425930743a051":"":"":"":"306b1f733e6f69b6f26b7baa5441af4967a5cad8faad18029440aa989aef6024dbf3b
a02dfc2c694dad6496ff760d72ae6914a4dcd5e3a443f4bcb14bf2b64986f35c32449f15e3084d46fadfa2ae213da6b26f
787cef89b6a23084a929608a9f6acd8315808c29f8ae435a40202a012"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-224,192+96,0,0) #8
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"78cdc1567caf2ff529ef8e3475c0fbb09a48b687a544f7399f503948621f29686fb15216":"":"":"":"2367067d8ec189b0819eda34602768a0698b4b545c7d5214fad58c9787b89809b97f3af5f9349907d2954f8c0dccbdbe63cc019bde3a6fae10497ae57f33e91ed55b6fc4a83fe8a2463552796d5120da8066f7285a8388958817b1218e006d7fc617f453ad0f9217966a0731ba99f093"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-224,192+96,0,0) #9
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"25f9ee24ee25ad3d29a974f8f552b178cb292b847a6be80694213a6c0b33e25e29fd3ecc":"":"":"":"32fe251a619d164c217365b12a313a942b6a9c3df007751a5fa9f356412d1142c785c292e3dc9d0b1d77e080892e5d39b91c58fd142458c71182061920a0721db453a32fe7ffc8b2c20bf11894fa37d8f0e9463edd43a97f65362295119be03d5e06f617fdff6accaab8c4da72ac8f81"

HMAC_DRBG NIST CAVS 14.3 No Reseed
(SHA-224,192+96,0,0) #10
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"0b644221788c266aae00a3b63a87f32ca96a6c32b116cd37caa4f75ff5d7e56be3b4e20f":"":"":"":"dc9245da77502cadd1a8ac4d1cf6a199c8e529deda10c87ab6c69ceea6fdef36d45f4d036021b93fe5b342c52fe1e71d81e617bebc58804af3109bab93dbb2e5c546e108bd0891710128b5e8e4a4f01df2003d038fec8cef426fad7f72dd5e091b4850e9bf4932d60deacb6e9ea3c5e6"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-224,192+96,0,0) #11
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"a6677badff70966a3cd2febaad7de7aa5849ba763789b20d0a39b6c569261b826cdb15e8":"":"":"":"e04838c970f5d7208a2a7310da893d65391666a5dc62d9ede71fc30816cfc3e8064ac59cc9aaf30283356078c812676ca20beb044a6d78db6c5ef9718a88559607f225002452c01459944433013cfffea84d6fe404fbbbc2d66bb50a2fa01d8a5d6e4ea9b402dc5256752461bf6fcb7f"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-224,192+96,0,0) #12
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"2301d8c053312db04882f4284cf8b47966c1c9b8c49de847d0c11f14c5f70ce19346562b":"":"":"":"b46246526b28f3ad7f6d8732ca3bfc40f005d97a519640a4ce728486d8bf830d661be5a97b11113e89096d9bf15cbef73ec28ac13e3fbeadc9bca500918bbe92ea23e131cc622dbffe2272db16ec5d4ca30e9bd986d1709ae22d10180514bcd11bd6218ea1fbaba101444945a17a4c4b"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-224,192+96,0,0) #13
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"78644ea1b0c4c55c4addeb476fc34471ea2c4393697aa4f170726010c443b8e1c4a6b3ea":"":"":"":"ef1b41bd03ee8460d55759db65a4c97758f48e3a09127be04c7ed08bbee5fa5cf119929df42c187e2a347a8df99c502b693a7ae41946f4918d84686880ae29d6d8fbbc4fccc9e295876a249cfa59effd331994e84717b4c76637df36beb960761880daab3d43376341439af2ce8e33cc"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-224,192+96,0,0) #14
depends_on:MBEDTLS_SHA256_C

hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"71acb71235e88e3aa6d8bbf27ccef8ef28043ebe8663f7bcf49cb642b3d915cf03b90e65":"":"":"":"144aeb56a11cb648b5ec7d40c2816e368426690db55b559f5633f856b79efe5f784944144756825b8fd7bf98beb758efe2ac1f650d54fc436a4bcd7dfaf3a66c192a7629eea8a357eef24b117a6e7d578797980eaefcf9a961452c4c1315119ca960ad08764fe76e2462ae1a191baeca"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-224,192+96,192,0) #0
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"c5c89c26ac4ca8b1106ba90a8ef4d6d687dfd88743caa5fbafa4745d9c1f8371120b10c8":"":"d3483ae5f9ed97efd3f852e4a6f20f25c947a03f39a4b75c":"2cd523c5958cdf403caa61abe5c4739cdb9d40152f0e769a":"1fef4e6abc2778d1c3e3ce00fdb5eae1ebebdd5cff0a7087644c8565d1e8b876b2c05264ca81498468851fc7b9e5a2163a06f377d2ed754c095adc59dc015a77edd69e4eecbe48d9dc127eedfff5cc73ae38127ae3a518fe7fa5abd1a9c53eeaf144420873341e2efa3d81493c69b04e"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-224,192+96,192,0) #1
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"6860e44bf582db9818ffbe4c699d4218965c29f463d7a02fe1f36c8442b0a5d103def7a2":"":"e9f598357109e2a532dc980388b8a5991256166d67c3bc01":"58ebbf7402be041724701e5c0132abe604c11a62a9de1d2f":"52fad34b27113c146595a6740f505bc2d3edf6618975cb9c4a5155788eaf08b96d232610d9b4ee06264fd92f319df5a52b8f9e31b016a6c21d27d31d9d42bbb7588a7142f26ece3ddf211c8cf4530947adee302aa71c0d7fe9060c1b25f1c1f2e053598a7fb72c4db55fb1b02352d60a"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-224,192+96,192,0) #2
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"27b9f78ae07821f2b5625c8fc3a03ceec4fc8062be860c2db20403dd88a8751dcad56158":"":"1b6c848fce706abd73612dd3fd421c1c7ce9f4c2d0ecc670":"14a43645c1b6ae394f795af6ca2e9084e7e707f3f2cedd7a":"33c592017af545b3a9cf3419ce1c604e9c7c687ebf6418fbef47ec96e61f1951068eec9b60005d24574313f04ffc16c30872ec83e41e248e3d5c6951930d6a88b8931d5502d1142ce50676b3adf48453d1a008189658db8511d19a06ac97b4d5cfac19b54e8e6b899d501715f401ef85"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-224,192+96,192,0) #3
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"8d7cf5c2e360ef755c1e9f5b7a44a1e29f09cee7ca44e15925ffe9a47b2d55fd7750b356":"":"0e691c9a435939c615f0686eae88e090ba5c4b3f5e6e00c0":"1e3a452295617e5a9e6f78256d2781feeb3812753b4aad9a":"a307569d8adf3f7e6ee4567a5b2bd338badb9234e7b27c92429ffa75e4c56c0529fdc6c15df5d47c46e3d2eeadcf1b9e93a5dd6cde99a82f04b0d97f7a3bfd05c0e1d8370987222310ab18c980ce48b2679361c3d9011dd355a9b06337c054ee37913d5f4dd30d1fc942cd733a0fa5f8"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-224,192+96,192,0) #4
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"1a0d2c734918c539c1b306a464eb6b54f92e958e8636032aec23ba8ae817bec48384461f":"":"b8ad9e613a891fd0db89571fddda77827382e406cd3cdf7e":"1e172a708aa4ffa3618ff0d7b1f9ba341f4811507851dfb4":"674df1f3095d6c87bc54dd9b2aaa2c786bd50e4ddc02493745d820dad8552131fb3e389e99b0709478b65d4268f2a3b468a8447dc572a6ee024be6be9be9d428c12cc92894d15dd1c959d6222dc9ec30478c7a0b57f5bd8bd53868b98d7674738b54cf74100ae215693babb6db3b3890"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-224,192+96,192,0) #5
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"95a30a0ca779a4038ea920cccfa4cdd814ca17d560d53a75cf170f4712994f9bcb2efb74":"":"1da6c8726bbfa3c8bee6dcff6f76f2d55d60527c4f0db26b":"595ebd903a596a1f12175080185bd94c2336eb8dd29a387d":"317c19cf4a45b8cf3f645da084ada54d1b1f81379152424fddad22a6dc9bd22841e0c4c5a36bfb7879eafbd1a939121905a938ae034c7fc01afb56607e35f895f46f13e91ce4e8e75b6a87a1e5544e18eb194fd6754b06885ac05e332a05ed436e889965e405e0f2069b04b40ea0f635"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-224,192+96,192,0) #6
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"8af8930562510231a592a72587fa6ad7c234e133046965907642fbc785c0b86cba844f0f":"":"9ee7b221064966582dc836437b82386f5204a302a4179079":"473d917f5b66f0f6e3fb4670ba08c2cbd2ea765b46b10838":"5c2fc9cc7148dbe40a692b3636778eb80188949d198bba3e8355386b78b54bfb963f5f2d9202988da20ccbf336a7c737a66c90149b9e8e306477151c4d912f7c61e872de0d0e47701cbe765864de536d599946b8bd65e4d89d4e61deb53de9974fbbe634501800feea100fea573e2e50"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-224,192+96,192,0) #7
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"2b9554ecf94c7d647a4e117f43326cab54466eba56a09a52741b2445057c491935c067d2":"":"0144be6978dba85aa645d793c1881dc2deb1bd210811ec9e":"1cd265f3812568274b643954c70923a76dfcc9f123360111":"f7459b0c23966dc1a53e0c6406c9e78ebe728e3484224cd88b6b2ea554522e75eb4a1c8a3fdc66561426464f50b8d0ff95b266677d91776b344a820eb4fd7d554678300558011a7cd85d22e92dc8ec2c2fa15c6330ba157c3e71728304447c1ad4d64f3da4fbf26d92e1e7c58a1b289c"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-224,192+96,192,0) #8
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"335ede8603fcde78ea9869da2dbcab4a6e72f1b53439f3085d06b856e627411a9ce1c297":"":"ededc73fe268935c10832c463549f8204a29cf0fe00a4d87":"ef1b8a80dd49d2c263999ddc0d5a1d9205c1b1c66239fd80":"05bfe97c398b1e33ee1c547c0edb5b654b7060b76604195440d06dd2f614a398c6c43f1803893c4c8888bedecdf998367cf992301a25f24c263f5d36bbfc6fe8b839cad293b3617c1d2c60a814bda0359e3f717fa80fc7324af8827d438c88642754b39b10d18cf5bf42f11177a0bc6b"

HMAC_DRBG NIST CAVS 14.3 No
Reseed (SHA-224,192+96,192,0) #9
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"9b0275d861117553ecd3c4d7cfe762f88df22c4c4190dac8e0be5872818e2dd765261d58":"":"cfc0b07082d514425b17ce3cb334ec62bc1b3be0be58ca4b":"d3c70ab5ff7a364a9e6dc75132ac67e0d373fa2df301afb5":"09fb41bcceb016e754795e1cce582f0cae91d7bb50245975eb75274819e1e4dcdfbc5e2f13fd26b9a9f9e945cd807ffec4e275681ea7bd33eae13efd8a01edbe02562e77b44b6312f416c3dd0be64f2bae0ba4b9bb36fc3a44841d21d8b3571c0ef644d88cf3cc3c851b256a15f4d716"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-224,192+96,192,0) #10
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"1981c3f9ca58fd10e8377a8d0eb3cf02102aab6f7a033af3135533d9fd850e29ecb8dc9b":"":"f9978ba41df22894ad5f3849c1bdf21f7bbc0128c782e79b":"b4d57de5e18d393273ee9f3ef9736599c6d639f437239219":"fee23db2fcc71624fb39f573e33a1490efc7230c27e9278188251634f9c045bcb26e79ec

e6a173491475ae44a957c4269570f5469234ca8b6873cc973c8d97178c58cec658a352bad0d4c6001cae5664258db59a
d76eb6304d166267eafb46f4dd536a914fa6d1ac58317e7c557d4653"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-224,192+96,192,0) #11
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"c10d4e521350f7cd1853576d03c4bece3e58c8c740859e4e16979
499ec1365fc073736a3":"":"78b245520153baacc66846e7a83a2a925f892d4c2ee63c0f":"c8ca7a33de5991d44d7ef7d
a2d3368cc2cdb93895c394d41":"f92c15f5833800b28dba2d134d4dcfc41abf72f5a700469551e8ccb83bdb0772d14d6
b26ba6978169e3ddbe5f214d57930dfcad719bf10d306749246d2624bedd4a18d327b8ae6bee67cf0bfb5f649824bbd0
440f042146b95a83e5845ced69a55ba055d5dfc7183c3bb28d61312d274"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-224,192+96,192,0) #12
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"7608b5617785995a1f7144ee5229e4f9c138e418bcc3b5e061a42
2e8cf875f58650e996d":"":"961c2d33039e60a2871e1f5b82097f6b1cb03836dba5f440":"b18cb52d3858ac5bf59f216
a28c0ad49f3dc88c67b5870e0":"4b0313ae873ce5ebf08aec160416492e4c4c797a5017061ea42aefa0685ab19b74a7af
11f019b9fb63072b797f7ea3354efd32c4abd1e866405a319ed2fa13fc81019d61326e70e503141b9c77b4879a45e9f36
f101dbfff4359147282ef814888fee81640def25f551cee41d12609aa"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-224,192+96,192,0) #13
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"fef7a43fea2ff1a0f624086985e535778d7a73dbc47bc23e9da92ed
d5d2f273cdbbc0251":"":"836731a57497a69e31f8db4f729774ad65f31d968dbc55a8":"bcca96d808ba98bb50e90afe5
8fc88e95dc14c3e90c56004":"4f2c64ecd146689064fbf4fcffce2a2ab3910e72ec4faec277f7b9e9ed510381312b01f216
50e175ebe9c45c11e977276f13be015243a0cd16a191abbac6462ba96e4e4a1120b28083da933419e8c8f03099906eb1
ee012ae291104c6530f51b5e32e6631cab8ef5aad68c0045255ba9"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-224,192+96,192,0) #14
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"00197c70b2f0d3e98e4b387ec42a65c4106a1689ab5de61101ee7
6f4b5e530e7efeaf964":"":"03015311cddd0961ec7a74cb84d835c058a69b964f18a1c1":"5e0d99e0e7c57769a43ea77
1c467fb5e2df6d06dae035fd6":"72e8ca7666e440ac6a84ab6f7be7e00a536d77315b119b49e5544bf3ead564bd06740f
09f6e20564542e0d597ac15a43b5fb5a0239a3362bc3a9efe1ce358ddd9d4f30b72e12ed9d78340c66b194beb4b12e97
3213931b9cfd0ccbdf540d2c36ce074e2beac7a4ddac59e06e4c7178d3"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-224,192+96,0,192) #0
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"c5c89c26ac4ca8b1106ba90a8ef4d6d687dfd88743caa5fbafa4745
d9c1f8371120b10c8":"":"d3483ae5f9ed97efd3f852e4a6f20f25c947a03f39a4b75c":"2cd523c5958cdf403caa61abe5c
4739cdb9d40152f0e769a":"1fef4e6abc2778d1c3e3ce00fdb5eae1ebebdd5cff0a7087644c8565d1e8b876b2c05264ca
81498468851fc7b9e5a2163a06f377d2ed754c095adc59dc015a77edd69e4eecbe48d9dc127eedfff5cc73ae38127ae3a5
18fe7fa5abd1a9c53eeaf144420873341e2efa3d81493c69b04e"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-224,192+96,0,192) #1
depends_on:MBEDTLS_SHA256_C

hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"6860e44bf582db9818ffbe4c699d4218965c29f463d7a02fe1f36c8442b0a5d103def7a2":"":"e9f598357109e2a532dc980388b8a5991256166d67c3bc01":"58ebbf7402be041724701e5c0132abe604c11a62a9de1d2f":"52fad34b27113c146595a6740f505bc2d3edf6618975cb9c4a5155788eaf08b96d232610d9b4ee06264fd92f319df5a52b8f9e31b016a6c21d27d31d9d42bbb7588a7142f26ece3ddf211c8cf4530947adee302aa71c0d7fe9060c1b25f1c1f2e053598a7fb72c4db55fb1b02352d60a"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-224,192+96,0,192) #2
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"27b9f78ae07821f2b5625c8fc3a03ceec4fc8062be860c2db20403dd88a8751dcad56158":"":"1b6c848fce706abd73612dd3fd421c1c7ce9f4c2d0ecc670":"14a43645c1b6ae394f795af6ca2e9084e7e707f3f2cedd7a":"33c592017af545b3a9cf3419ce1c604e9c7c687ebf6418fbef47ec96e61f1951068eec9b60005d24574313f04ffc16c30872ec83e41e248e3d5c6951930d6a88b8931d5502d1142ce50676b3adf48453d1a008189658db8511d19a06ac97b4d5cfac19b54e8e6b899d501715f401ef85"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-224,192+96,0,192) #3
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"8d7cf5c2e360ef755c1e9f5b7a44a1e29f09cee7ca44e15925ffe9a47b2d55fd7750b356":"":"0e691c9a435939c615f0686eae88e090ba5c4b3f5e6e00c0":"1e3a452295617e5a9e6f78256d2781feeb3812753b4aad9a":"a307569d8adf3f7e6ee4567a5b2bd338badb9234e7b27c92429ffa75e4c56c0529fdc6c15df5d47c46e3d2eeadcf1b9e93a5dd6cde99a82f04b0d97f7a3bfd05c0e1d8370987222310ab18c980ce48b2679361c3d9011dd355a9b06337c054ee37913d5f4dd30d1fc942cd733a0fa5f8"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-224,192+96,0,192) #4
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"1a0d2c734918c539c1b306a464eb6b54f92e958e8636032aec23ba8ae817bec48384461f":"":"b8ad9e613a891fd0db89571fddda77827382e406cd3cdf7e":"1e172a708aa4ffa3618ff0d7b1f9ba341f4811507851dfb4":"674df1f3095d6c87bc54dd9b2aaa2c786bd50e4ddc02493745d820dad8552131fb3e389e99b0709478b65d4268f2a3b468a8447dc572a6ee024be6be9be9d428c12cc92894d15dd1c959d6222dc9ec30478c7a0b57f5bd8bd53868b98d7674738b54cf74100ae215693babb6db3b3890"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-224,192+96,0,192) #5
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"95a30a0ca779a4038ea920cccfa4cdd814ca17d560d53a75cf170f4712994f9bcb2efb74":"":"1da6c8726bbfa3c8bee6dcff6f76f2d55d60527c4f0db26b":"595ebd903a596a1f12175080185bd94c2336eb8dd29a387d":"317c19cf4a45b8cf3f645da084ada54d1b1f81379152424fddad22a6dc9bd22841e0c4c5a36bfb7879eafbd1a939121905a938ae034c7fc01afb56607e35f895f46f13e91ce4e8e75b6a87a1e5544e18eb194fd6754b06885ac05e332a05ed436e889965e405e0f2069b04b40ea0f635"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-224,192+96,0,192) #6
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"8af8930562510231a592a72587fa6ad7c234e1330469659076 42fbc785c0b86cba844f0f":"":"9ee7b221064966582dc836437b82386f5204a302a4179079":"473d917f5b66f0f6e3fb4670ba08c2cbd2ea765b46b10838":"5c2fc9cc7148dbe40a692b3636778eb80188949d198bba3e8355386b78b54bfb963f5f2d9202988da20ccbf336a7c737a66c90149b9e8e306477151c4d912f7c61e872de0d0e47701cbe765864de536d599946b8bd65e4d89d4e61deb53de9974fbbe634501800feea100fea573e2e50"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-224,192+96,0,192) #7
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"2b9554ecf94c7d647a4e117f43326cab54466eba56a09a52741b2445057c491935c067d2":"":"0144be6978dba85aa645d793c1881dc2deb1bd210811ec9e":"1cd265f3812568274b643954c70923a76dfcc9f123360111":"f7459b0c23966dc1a53e0c6406c9e78ebe728e3484224cd88b6b2ea554522e75eb4a1c8a3fdc66561426464f50b8d0ff95b266677d91776b344a820eb4fd7d554678300558011a7cd85d22e92dc8ec2c2fa15c6330ba157c3e71728304447c1ad4d64f3da4fbf26d92e1e7c58a1b289c"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-224,192+96,0,192) #8
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"335ede8603fcde78ea9869da2dbcab4a6e72f1b53439f3085d06b856e627411a9ce1c297":"":"ededc73fe268935c10832c463549f8204a29cf0fe00a4d87":"ef1b8a80dd49d2c263999ddc0d5a1d9205c1b1c66239fd80":"05bfe97c398b1e33ee1c547c0edb5b654b7060b76604195440d06dd2f614a398c6c43f1803893c4c8888bedecdf998367cf992301a25f24c263f5d36bbfc6fe8b839cad293b3617c1d2c60a814bda0359e3f717fa80fc7324af8827d438c88642754b39b10d18cf5bf42f11177a0bc6b"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-224,192+96,0,192) #9
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"9b0275d861117553ecd3c4d7cfe762f88df22c4c4190dac8e0be5872818e2dd765261d58":"":"cfc0b07082d514425b17ce3cb334ec62bc1b3be0be58ca4b":"d3c70ab5ff7a364a9e6dc75132ac67e0d373fa2df301afb5":"09fb41bcceb016e754795e1cce582f0cae91d7bb50245975eb75274819e1e4dcdfbc5e2f13fd26b9a9f9e945cd807ffec4e275681ea7bd33eae13efd8a01edbe02562e77b44b6312f416c3dd0be64f2bae0ba4b9bb36fc3a44841d21d8b3571c0ef644d88cf3cc3c851b256a15f4d716"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-224,192+96,0,192) #10
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"1981c3f9ca58fd10e8377a8d0eb3cf02102aab6f7a033af3135533d9fd850e29ecb8dc9b":"":"f9978ba41df22894ad5f3849c1bdf21f7bbc0128c782e79b":"b4d57de5e18d393273ee9f3ef9736599c6d639f437239219":"fee23db2fcc71624fb39f573e33a1490efc7230c27e9278188251634f9c045bcb26e79ece6a173491475ae44a957c4269570f5469234ca8b6873cc973c8d97178c58cec658a352bad0d4c6001cae5664258db59ad76eb6304d166267eafb46f4dd536a914fa6d1ac58317e7c557d4653"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-224,192+96,0,192) #11
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"c10d4e521350f7cd1853576d03c4bece3e58c8c740859e4e16979499ec1365fc073736a3":"":"78b245520153baacc66846e7a83a2a925f892d4c2ee63c0f":"c8ca7a33de5991d44d7ef7da2d3368cc2cdb93895c394d41":"f92c15f5833800b28dba2d134d4dcfc41abf72f5a700469551e8ccb83bdb0772d14d6b26ba6978169e3ddbe5f214d57930dfcad719bf10d306749246d2624bedd4a18d327b8ae6bee67cf0bfb5f649824bbd0440f042146b95a83e5845ced69a55ba055d5dfc7183c3bb28d61312d274"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-224,192+96,0,192) #12
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"7608b5617785995a1f7144ee5229e4f9c138e418bcc3b5e061a422e8cf875f58650e996d":"":"961c2d33039e60a2871e1f5b82097f6b1cb03836dba5f440":"b18cb52d3858ac5bf59f216

a28c0ad49f3dc88c67b5870e0":"4b0313ae873ce5ebf08aec160416492e4c4c797a5017061ea42aefa0685ab19b74a7af11f019b9fb63072b797f7ea3354efd32c4abd1e866405a319ed2fa13fc81019d61326e70e503141b9c77b4879a45e9f36f101dbfff4359147282ef814888fee81640def25f551cee41d12609aa"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-224,192+96,0,192) #13
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"fef7a43fea2ff1a0f624086985e535778d7a73dbc47bc23e9da92edd5d2f273cdbbc0251":"":"836731a57497a69e31f8db4f729774ad65f31d968dbc55a8":"bcca96d808ba98bb50e90afe58fc88e95dc14c3e90c56004":"4f2c64ecd146689064fbf4fcffce2a2ab3910e72ec4faec277f7b9e9ed510381312b01f21650e175ebe9c45c11e977276f13be015243a0cd16a191abbac6462ba96e4e4a1120b28083da933419e8c8f03099906eb1ee012ae291104c6530f51b5e32e6631cab8ef5aad68c0045255ba9"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-224,192+96,0,192) #14
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"00197c70b2f0d3e98e4b387ec42a65c4106a1689ab5de61101ee76f4b5e530e7efeaf964":"":"03015311cddd0961ec7a74cb84d835c058a69b964f18a1c1":"5e0d99e0e7c57769a43ea771c467fb5e2df6d06dae035fd6":"72e8ca7666e440ac6a84ab6f7be7e00a536d77315b119b49e5544bf3ead564bd06740f09f6e20564542e0d597ac15a43b5fb5a0239a3362bc3a9efe1ce358ddd9d4f30b72e12ed9d78340c66b194beb4b12e973213931b9cfd0ccbdf540d2c36ce074e2beac7a4ddac59e06e4c7178d3"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-224,192+96,192,192) #0
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"e4547261c9dda6bafe9fddf435a80ebc96354c7c2c8847c5d26c6e73a967bfc4ebaf8613":"42849dc8eec611eaa49252067fa60d7d7267d711dc35b576":"815f50fc233f157f96ad0627c355bce407b269dca91af661":"775a1c9da6f58d4eb95b27935ecc01dde31ff17ce2e4e65d":"25adb777523a80a6dbb6ac1fd08e02bfc4b4686cec5efe3ae9aa2d4469eae8c9c3693fdc8e0fc107720b7789ef7331e23fe3799412ec86857ffbba515a5af4d91013b2f17669421c822005b4747942790a11a24c4974f27d54de69727b0ed507b6a48a9d6c53f93e2f3d33df73dd643f"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-224,192+96,192,192) #1
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"06d677001d9b3c97fda4d09778aee3de131b4123696b109f81bb6b0d7fbcab3c5842bb83":"f99638d2d4365b662cd83ab4e6a7bbb624e6c72b7b38e81b":"20b7d56f6222bafeeeee59dbca1933d8086218891f3a9bfe":"9de4f2847fe239cb1a3df4b8ff64c25d7b0870f3c9ebe3a3":"e18ff19837ce21e68944659321311b8584dd515ed8a6a1f2b0ac06e69009c3d0cf0489af876201efad962cfd1ba54f540b94131d788d3fea797c4bc079593bc7932baa70abb145a355741a98c584f0fa3298b8310b01e1a6debf5359d7d02b1a6c663100acb56975450bec20e91b736b"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-224,192+96,192,192) #2
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"abd38c0465cdfe018f36ffbb7a0ee51d67675ab4f0f1d1e93418bb4cdf6499a371af4d3a":"9a07d5571d841e3c1a9eb3fb48cde3b3e080e1c2e0db6a6d":"a392f79022aebbec0c82b981293627d139dfb5232eb490b4":"f5ce1f6b1e6715c49bea42ff439fdecd9b3b7f2e578133cc":"885c54ad25992fc38260498d6f4d8c73d6159af5f7efef06174da03afcd8384cb28690fd9ded1d26e2dff74aee4dd0c47a0d99c6fc1ec8d8faccbdcf6fdb12a528564ad0d8131bcf5222d7e6c69c52da1acba01b721c98ac5a33725111f12f6d8100009d7cc9efb7ad8d7d95ea4e62

0d"

HMAC_DRBG NIST CAVS 14.3 No
Reseed (SHA-224,192+96,192,192) #3
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"b52620e58e0b52b8eed0d6a6c5f4ff6c1483c61fc41dacf72bf475b37d068d061d1edcea":"ef0d233de00d24622b7d4ff4215aa720787fe80aaeb65d7a":"81b735acd3dcb13e65231c2d980fb40ca850370581f230d2":"b2302d024d92cdaed4b12f79b0aeb20c98b2321710fefab2":"ae94204670196baf740768f97b3a095134b384afea667fd90a77a16c8ae390a732ff49a3073a27db0f7a2c8ad5d7cb527d334a37abf0472f292a20f2a28e667d7c9e9f7b8fbdd177f36bf92d66223aee3f712b6c9b064e07ab96f6a77613ea55008fb4f8fbcb2f1ccbb0da75316c1faa"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-224,192+96,192,192) #4
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"2592a5ed86ff64b9b4c1fbb81222d1bfbc53f3a639571ecc356084058b8855237da15c50":"a626c51ec99e72431485d2ba027ed9cabcae7b86116abe4f":"c430876552d28776570923c6b74e42c3210f01104006bf11":"fe2ebc239690a4eb18a0b5e75d08831cc2eb07c982c63973":"005045ade7cc15467b5ea784649d9804540a842ffba4db8d44df4f44c69480bd4fe965b645aed09d62190daeb2693a2192aec3d71453a8218e4700201ab922ac35d241d95150b47cc7a051897be4d958f2da5c2ebbfceb1c550cb67b32ff83ce4fd845fd826a0d2469b506f5158765fa"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-224,192+96,192,192) #5
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"376785f5ff8a82ceb0aaeb010533cc1089059ec583c302b14bc47e2cb8c2711839ce7f68":"6d345e248339e893f75696c039ac47e5678696fd489a393c":"b0f3fa1131c3fdd5c7fd2de93931e45a66fa030422ac65db":"c66341e3f9fb82e3ba85f229fcb7d34457e4a6ba8396b548":"b92d17e1be94b0385a8cc3e16189811fef7b284a1b0b6b2520fde79af7826c745e746486a70cd8dd9930b163da75f7eea7c216e758d9ed6c745dcd7bde19bb9382c1f7c37cd15b703b884d7d452c255b25048a836844c5ff28aaacf733a52c28904b36e1b51729d7aed81d601c0872dd"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-224,192+96,192,192) #6
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"2cc2557582c5a90cd2ad0c4a5578eb0bbc9bde41b126e46d8e9c3563341ba238414eb628":"9d2fbb9153e3ffefae0770c79de10db069a5ff9f50e31787":"2e54e32539e27ef76ac1eeae2e30c2385647652e20903b39":"1f4e01255908c3c8049521f8972c01ede7dc76c425c59640":"7d6ccdfab33f322898c470be02d8257e0e952dd10f407b3a8eaeeba47c541d968d79eca29e15541c1505fe4f19a41797c9ca2280c06261fe9d0c58bab65d16f5794b57566b8795c38c7b43d4761c8fd107beb95147a0fe61ae8dc31e25eb2957e44c0463ca7c1b589ea587f0cae1428c"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-224,192+96,192,192) #7
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"e670f896326b76034e43cd85f6f6f11fe6582d3471a8eb88d37a2302de010aac0e556860":"5e218091abee1960ef81f4d5a80415e388bd0cc79bed70cf":"7cf84b9ff30dbd0f608fb21646d7c5b542fba50adb38d5df":"c1c4aabe7616a4c97a4dbdadb08a9b63c6e10cef8d463fd8":"d8fbd557fccf31829b5ee11b05d0353e725bff15fdaac94d21ce95d40eff55edd852b264b515ec6384e2d28d014e47a2df0d4f56a4ec79309b06affc62915e231d62d02bfc60220c72b7ca7ba5671f882839b791ef534e707a04e5274c1011f7941fe1075a5d06a47af9fb2f65c1

f211"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-224,192+96,192,192) #8
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"0576bb2d4c663b781193509251e2f76b0a8bb792e79449600c2c154feb70cf33ca942508":"ad15e4fce9f4dea43c12ff9f9d50c963b335a01332541154":"3c8a4d6ab96cebf9d02b5663dcb0e0db23699623455cd4b5":"43d2d3a8d023fa1785ce4781a15eb20ad787685a47da08f0":"a68e648cb07da2eb795a8c898c8631e565f33c2fe9c35e686d6f85fef145446cb79bb6d17bdc8224bfe437468a9630ed03c517caf1226c278ae510c869d67d50b6bf1cb378a34035041f290d8dbc123650ab4fbe5cf6074ed0ba90e45d9a8ae08566ea3d3a00ee3741c8ec8f56dcc78c"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-224,192+96,192,192) #9
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"f597ce05b9a5b1cf3847bbd4171e5085384cc256f77ac61573b435726cbd538b93de9f55":"573cf859f8fea05f16c6d03cb4e524b91e917f39eeeb1d68":"2a842454870c3f7936f8036b453d219557ca341f261d2519":"7afd8cc269899acd88f5c55af29fb0c4ce678a0d8ebf924f":"8162c16c1ce3d5c6b7c96f0281f4220569a882277935752b86e7d3f54646b276cb77ed96da73799911fca3d19d34c1f0b21068a472afcb77410412eff2abd03c753a009ce02b0e995477546366020294eff0ef0da66f31a413313e2774ca04f09a4d5076e0e85ca97d5bb6faac4c0c27"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-224,192+96,192,192) #10
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"d5b5374fe143035c4fea41667bc8bc7d46000998cc82ab32a0040c705e01f9b354e8f16e":"ed8bb219e67515874c5b9e3f6ae6e4dfa9c42d1e69204e8b":"70f03fe6e78cc34ec1678b2708fcd8ae3300183ea15ccfc7":"9c641d7e73d1a2b819e113747d74a979b74c444ed36b7391":"d50df8e3e17c0f5e19673ba2097d1d0c4cf7a9def7465a5b91ac8d49ae1b6a821fe9efde841ec9064555c0e2d6cdfa41f1089f22a5c27090c5a136660d1af586a1e131a853f19bc3c8f4c79aa09e39c2f22b4456c667ec907e2a4124218665e7cce50399ae1e19ba9c2399f470444839"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-224,192+96,192,192) #11
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"74d7c8c9b170e59e4f128c8df1955838df5c8071a5e85439d71e785c68b37e10efb39c9a":"be3d54203a1078d051519137774d5d851e81be026155eb78":"23f7b6758d79de580ed3eb995fc173da74939837aa8d9eb4":"6f0d5a333ddea0d38362df0dc3ebaa2be2fe5825ddb0ce84":"4462fc32110b25b3797c5cafaad830e8a4346d9270fed98b30f1345a7a8dde19bf5365d6f3788e7f715feb2762af263839c8c8188908c61120743d977d71c51f6324d887bbda380fc07eff09a31c2332e7b1aa1692c59c3379db95fc21cf711c004c4d385fe14f48f2f2a31bcce6aaec"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-224,192+96,192,192) #12
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"eaf27c3f69279fd523c0c3a1da5fc4f01ed64c27ffcfe3c1c596482f5baae1434e8c687c":"b038829fc95dcba8645ce40a306491c893f48139ae30a071":"fbbf7abb8cc2612eeea6d9463efd55c47245e01713332bd6":"ccd7e81f529de1ff4e65fc63d34c262ffde7ee49e6707197":"96dfb7445057633b2f0deb69135d10d0a2dc53faa9cded55ddfb8edc63f5424f8fec7627597a30328177dde7963f76f9e5412b5b440256c6a3f0c7c7fa02ca49e19ea176abac013696e9d529f65e51d4a7348e42dd254bbf19d9632d6c875b8ecd7a4139f1bf020a159d2a30af8d6

45f"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-224,192+96,192,192) #13
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"319cbf2b11b37c831c654b6cec2570dc6d7abeeab185272a518eaef30faa5acf5c8b254d":"9effa141f7466b659eaa50c32c8e683c2640f54027ab6aa5":"63b3acc237588cdf41c0d4bef16c4890cf3d458fcf1de8ea":"573d6a7960aeccc3280a8aee4d72e587e9d196b7b270e329":"8a568086fdd9f01206a5aaee34d253bbc9339112d3170699b9a1392e97062d5d0f16240114dc1789269217c5b4b2974895b20903890f7dacfef46fa4a4d02891c70425ab3b42f53d72f852faf3713ac7b8207dc453279f4df345091b8bfeb54983095c2d190358293ba507bdfdc39b24"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-224,192+96,192,192) #14
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA224:"56f3f5b08da10ead0c986dd2ae5553e4b2eeeb47ad5d22197b12b89b4a871c51c0d85554":"96c8630a1f4187fb0794601cf51e7e333e71756a0421ff43":"875e5bc9548917a82b6dc95200d92bf4218dba7ab316a5fe":"4d3f5678b00d47bb9d0936486de60407eaf1282fda99f595":"90969961ef9283b9e600aead7985455e692db817165189665f498f219b1e5f277e586b237851305d5205548b565faeb02bb7b5f477c80ba94b0563e24d9309d2957a675848140f5601f698459db5899b20dda68f000ccb18dcd39dfae49955b8478fd50bb59d772045beb338622efa5a"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-256,256+128,0,0) #0
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"ca851911349384bffe89de1cbdc46e6831e44d34a4fb935ee285dd14b71a7488659ba96c601dc69fc902940805ec0ca8":"":"":"":"e528e9abf2dece54d47c7e75e5fe302149f817ea9fb4bee6f4199697d04d5b89d54fbb978a15b5c443c9ec21036d2460b6f73ebad0dc2aba6e624abf07745bc107694bb7547bb0995f70de25d6b29e2d3011bb19d27676c07162c8b5ccde0668961df86803482cb37ed6d5c0bb8d50cf1f50d476aa0458bdaba806f48be9dcb8"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-256,256+128,0,0) #1
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"79737479ba4e7642a221fcfd1b820b134e9e3540a35bb48ffae29c20f5418ea33593259c092bef4129bc2c6c9e19f343":"":"":"":"cf5ad5984f9e43917aa9087380dac46e410ddc8a7731859c84e9d0f31bd43655b924159413e2293b17610f211e09f770f172b8fb693a35b85d3b9e5e63b1dc252ac0e115002e9bedfb4b5b6fd43f33b8e0eafb2d072e1a6fee1f159df9b51e6c8da737e60d5032dd30544ec51558c6f080bdbdab1de8a939e961e06b5f1aca37"

HMAC_DRBG NIST
CAVS 14.3 No Reseed (SHA-256,256+128,0,0) #2
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"b340907445b97a8b589264de4a17c0bea11bb53ad72f9f33297f05d2879d898d65cb27735d83c0708f72684ea58f7ee5":"":"":"":"75183aaaf3574bc68003352ad655d0e9ce9dd17552723b47fab0e84ef903694a32987eeddbdc48efd24195dbdac8a46ba2d972f5808f23a869e71343140361f58b243e62722088fe10a98e43372d252b144e00c89c215a76a121734bdc485486f65c0b16b8963524a3a70e6f38f169c12f6cbdd169dd48fe4421a235847a23ff"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-256,256+128,0,0) #3

depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"8e159f60060a7d6a7e6fe7c9f769c30b98acb1240b25e7ee33f1da834c0858e7c39d35052201bdcce4e127a04f04d644":"":"":"":"62910a77213967ea93d6457e255af51fc79d49629af2fccd81840cdfbb4910991f50a477cbd29edd8a47c4fec9d141f50dfde7c4d8fcab473eff3cc2ee9e7cc90871f180777a97841597b0dd7e779eff9784b9cc33689fd7d48c0dcd341515ac8fecf5c55a6327aea8d58f97220b7462373e84e3b7417a57e80ce946d6120db5"

HMAC_DRBG NIST CAVS 14.3
No Reseed (SHA-256,256+128,0,0) #4
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"74755f196305f7fb6689b2fe6835dc1d81484fc481a6b8087f649a1952f4df6ac36387a544a5f2b78007651a7b74b749":"":"":"":"b2896f3af4375dab67e8062d82c1a005ef4ed119d13a9f18371b1b873774418684805fd659bfd69964f83a5cfe08667ddad672cafd16befffa9faed49865214f703951b443e6dca22edb636f3308380144b9333de4bcb0735710e4d9266786342fc53babe7bdbe3c01a3addb7f23c63ce2834729fabbd419b47beceb4a460236"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-256,256+128,0,0) #5
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"4b222718f56a3260b3c2625a4cf80950b7d6c1250f170bd5c28b118abdf23b2f7aed52d0016fcaef0b6492bc40bbe0e9":"":"":"":"a6da029b3665cd39fd50a54c553f99fed3626f4902ffe322dc51f0670dfe8742ed48415cf04bbad5ed3b23b18b7892d170a7dcf3ef8052d5717cb0c1a8b3010d9a9ea5de70ae5356249c0e098946030c46d9d3d209864539444374d8fbcae068e1d6548fa59e6562e6b2d1acbda8da0318c23752ebc9be0c1c1c5b3cf66dd967"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-256,256+128,0,0)
#6
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"b512633f27fb182a076917e39888ba3ff35d23c3742eb8f3c635a044163768e0e2c39b84629a3de5c301db5643af1c21":"":"":"":"fb931d0d0194a97b48d5d4c231fdad5c61aedf1c3a55ac24983ecbf38487b1c93396c6b86ff3920cfa8c77e0146de835ea5809676e702dee6a78100da9aa43d8ec0bf5720befa71f82193205ac2ea403e8d7e0e6270b366dc4200be26afd9f63b7e79286a35c688c57cbff55ac747d4c28bb80a2b2097b3b62ea439950d75dff"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-256,256+128,0,0) #7
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"aae3ffc8605a975befefcea0a7a286642bc3b95fb37bd0eb0585a4cabf8b3d1e9504c3c0c4310c1c0746a036c91d9034":"":"":"":"2819bd3b0d216dad59ddd6c354c4518153a2b04374b07c49e64a8e4d055575dfbc9a8fcde68bd257ff1ba5c6000564b46d6dd7ecd9c5d684fd757df62d85211575d3562d7814008ab5c8bc00e7b5a649eae2318665b55d762de36eba00c2906c0e0ec8706edb493e51ca5eb4b9f015dc932f262f52a86b11c41e9a6d5b3bd431"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-256,256+128,0,0)
#8
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"b9475210b79b87180e746df704b3cbc7bf8424750e416a7fbb5ce3ef25a82cc624baf03599c10df6ef44065d715a93f7":"":"":"":"ae12d784f796183c50db5a1a283aa35ed9a2b685dacea97c596ff8c294906d1b1305ba1f80254eb062b874a8dfffa3378c809ab2869aa51a4e6a489692284a25038908a347342175c38401193b8afc498077e10522bec5c70882b7f760ea5946870bd9fc72961eedbe8bff4fd58c7cc1589bb4f369ed0d3bf

26c5bbc62e0b2b2"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-256,256+128,0,0) #9
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"27838eb44ceccb4e36210703ebf38f659bc39dd3277cd76b7a9bc
d6bc964b62839cfe0210db2e7b0eb52a387476e7ea1":"":"":"":"e5e72a53605d2aaa67832f97536445ab774dd9bff7f13
a0d11fd27bf6593bfb52309f2d4f09d147192199ea584503181de87002f4ee085c7dc18bf32ce5315647a3708e6f404d6
588c92b2dda599c131aa350d18c747b33dc8eda15cf40e95263d1231e1b4b68f8d829f86054d49cfdb1b8d96ab046511
0569c8583a424a099a"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-256,256+128,0,0) #10
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"d7129e4f47008ad60c9b5d081ff4ca8eb821a6e4deb91608bf4e26
47835373a5a72882773f78c2fc4878295840a53012":"":"":"":"0cbf48585c5de9183b7ff76557f8fc9ebcfdfde07e588a8
641156f61b7952725bbee954f87e9b937513b16bba0f2e523d095114658e00f0f3772175acfcb3240a01de631c19c5a83
4c94cc58d04a6837f0d2782fa53d2f9f65178ee9c837222494c799e64c60406069bd319549b889fa00a0032dd7ba5b1cc
9edbf58de82bfcd"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-256,256+128,0,0) #11
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"67fe5e300c513371976c80de4b20d4473889c9f1214bce718bc32
d1da3ab7532e256d88497738a33923aa003a8d7845c":"":"":"":"b44660d64ef7bcebc7a1ab71f8407a02285c7592d755
ae6766059e894f694373ed9c776c0cfc8594413eefb400ed427e158d687e28da3ecc205e0f7370fb089676bbb0fa591ec
8d916c3d5f18a3eb4a417120705f3e2198154cd60648dbfcfc901242e15711cacd501b2c2826abe870ba32da785ed6f1f
dc68f203d1ab43a64f"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-256,256+128,0,0) #12
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"de8142541255c46d66efc6173b0fe3ffaf5936c897a3ce2e9d5835
616aafa2cbd01f9002c407127bc3297a561d89b81d":"":"":"":"64d1020929d74716446d8a4e17205d0756b526486781
1aa24d0d0da8644db25d5cde474143c57d12482f6bf0f31d10af9d1da4eb6d701bdd605a8db74fb4e77f79aaa9e450afd
a50b18d19fae68f03db1d7b5f1738d2fdce9ad3ee9461b58ee242daf7a1d72c45c9213eca34e14810a9fca5208d5c56d80
66bab1586f1513de7"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-256,256+128,0,0) #13
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"4a8e0bd90bdb12f7748ad5f147b115d7385bb1b06aee7d8b76136
a25d779bcb77f3cce4af8c8ce3c45bdf23c6b181a00":"":"":"":"320c7ca4bbeb7af977bc054f604b5086a3f237aa550165
8112f3e7a33d2231f5536d2c85c1dad9d9b0bf7f619c81be4854661626839c8c10ae7fdc0c0b571be34b58d66da55367
6167b00e7d8e49f416aacb2926c6eb2c66ec98bffae20864cf92496db15e3b09e530b7b9648be8d3916b3c20a3a779bec
7d66da63396849aaf"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-256,256+128,0,0) #14
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"451ed024bc4b95f1025b14ec3616f5e42e80824541dc795a2f075
00f92adc6652f28e6ee8de5879db1eccd58c994e5f0":"":"":"":"3fb637085ab75f4e95655faae95885166a5fbb423bb03d

bf0543be063bcd48799c4f05d4e522634d9275fe02e1edd920e26d9accd43709cb0d8f6e50aa54a5f3bdd618be23cf73ef736ed0ef7524b0d14d5bef8c8aec1cf1ed3e1c38a808b35e61a44078127c7cb3a8fd7addfa50fcf3ff3bc6d6bc355d5436fe9b71eb44f7fd"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-256,256+128,0,256) #0
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"d3cc4d1acf3dde0c4bd2290d262337042dc632948223d3a2eaab87da44295fbd0109b0e729f457328aa18569a9224921":"":"3c311848183c9a212a26f27f8c6647e40375e466a0857cc39c4e47575d53f1f6":"fcb9abd19ccfbccef88c9c39bfb3dd7b1c12266c9808992e305bc3cff566e4e4":"9c7b758b212cd0fcecd5daa489821712e3cdea4467b560ef5ddc24ab47749a1f1ffdbbb118f4e62fcfca3371b8fbfc5b0646b83e06bfbbab5fac30ea09ea2bc76f1ea568c9be0444b2cc90517b20ca825f2d0eccd88e7175538b85d90ab390183ca6395535d34473af6b5a5b88f5a59ee7561573337ea819da0dcc3573a22974"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-256,256+128,0,256) #1
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"f97a3cfd91faa046b9e61b9493d436c4931f604b22f1081521b3419151e8ff0611f3a7d43595357d58120bd1e2dd8aed":"":"517289afe444a0fe5ed1a41dbbb5eb17150079bdd31e29cf2ff30034d8268e3b":"88028d29ef80b4e6f0fe12f91d7449fe75062682e89c571440c0c9b52c42a6e0":"c6871cff0824fe55ea7689a522298867304 50e5d362da5bf590dcf9acd67fed4cb32107df5d03969a66b1f6494fdf5d63d5b4d0d34ea7399a07d0116126d0d518c7c55ba46e12f62efc8fe28a51c9d428e6d371d7397ab319fc73ded4722e5b4f30004032a6128df5e7497ecf82ca7b0a50e867ef6728a4f509a8c859087039c"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-256,256+128,0,256) #2
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"0f2f23d64f481cabec7abb01db3aabf125c3173a044b9bf26844300b69dcac8b9a5ae13232b43aa19cfe8d7958b4b590":"":"ec4c7a62acab73385f567da10e892ff395a0929f959231a5628188ce0c26e818":"6b97b8c6b6bb8935e676c410c17caa8042aa3145f856d0a32b641e4ae5298648":"7480a361058bd9afa3db82c9d7586e42269102013f6ec5c269b6d05f17987847748684766b44918fd4b65e1648622fc0e0954178b0279dfc9fa99b66c6f53e51c4860131e9e0644287a4afe4ca8e480417e070db68008a97c3397e4b320b5d1a1d7e1d18a95cfedd7d1e74997052bf649d132deb9ec53aae7dafdab55e6dae93"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-256,256+128,0,256) #3
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"53c56660c78481be9c63284e005fcc14fbc7fb27732c9bf1366d01a426765a31dc7a14d0eb5b0b3534e717a0b3c64614":"":"3aa848706ecb877f5bedf4ffc332d57c22e08747a47e75cff6f0fd1316861c95":"9a401afa739b8f752fddacd291e0b854f5eff4a55b515e20cb319852189d3722":"5c0eb420e0bf41ce9323e815310e4e8303cd677a8a8b023f31f0d79f0ca15aeb636099a369fd074d69889865eac1b72ab3cbfebdb8cf460b00072802e2ec648b1349a5303be4ccaadd729f1a9ea17482fd026aaeb93f1602bc1404b9853adde40d6c34b844cf148bc088941ecfc1642c8c0b9778e45f3b07e06e21ee2c9e0300"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-256,256+128,0,256) #4
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"f63c804404902db334c54bb298fc271a21d7acd9f770278e089775710bf4fdd73e45009ea9cb2a36ba1aa4bf39178200":"":"d165a13dc8cc43f3f0952c3f5d3de4136954d983683d4a3e6d2dc4c89bf23423":"75106bc86d0336df85097f6af8e80e2da59046a03fa65b06706b8bbc7ffc6785":"6363139bba32c22

a0f5cd23ca6d437b5669b7d432f786b8af445471bee0b2d24c9d5f2f93717cbe00d1f010cc3b9c515fc9f7336d53d4d26
ba5c0d76a90186663c8582eb739c7b6578a3328bf68dc2cec2cd89b3a90201f6993adcc854df0f5c6974d0f5570765a15
fe03dbce28942dd2fd16ba2027e68abac83926969349af8"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-256,256+128,0,256) #5
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"2aaca9147da66c176615726b69e3e851cc3537f5f279fe7344233d
8e44cfc99d4e171f080af9a6081bee9f183ac9e340":"":"d75a2a6eb66c3833e50f5ec3d2e434cf791448d618026d0c360
806d120ded669":"b643b74c15b37612e6577ed7ca2a4c67a78d560af9eb50a4108fca742e87b8d6":"501dcdc977f4ba8
56f24eaa4968b374bebb3166b280334cb510232c31ebffde10fa47b7840ef3fe3b77725c2272d3a1d4219baf23e0290c6
22271edcced58838cf428f0517425d2e19e0d8c89377eecfc378245f283236fafa466c914b99672ceafab369e8889a0c86
6d8bd639db9fb797254262c6fd44cfa9045ad6340a60ef"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-256,256+128,0,256) #6
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"a2e4cd48a5cf918d6f55942d95fcb4e8465cdc4f77b7c52b6fae5b1
6a25ca306bef036716440db6e6d333d9d760b7ca8":"":"bfa591c7287f3f931168f95e38869441d1f9a11035ad8ea625b
b61b9ea17591c":"c00c735463bca215adc372cb892b05e939bf669583341c06d4e31d0e5b363a37":"e7d136af69926a
5421d4266ee0420fd729f2a4f7c295d3c966bdfa05268180b508b8a2852d1b3a06fd2ab3e13c54005123ef319f42d0c6d
3a575e6e7e1496cb28aacadbcf83740fba8f35fcee04bb2ed8a51db3d3362b01094a62fb57e33c99a432f29fce6676cffbb
cc05107e794e75e44a02d5e6d9d748c5fbff00a0178d65"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-256,256+128,0,256) #7
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"95a67771cba69011a79776e713145d309edae56fad5fd6d41d83e
aff89df6e5ebe5b5164e31ecc51ba6f7c3c5199eb33":"":"065f693b229a7c4fd373cd15b3807552dd9bf98c5485cef361
949d4e7d774b53":"9afb62406f0e812c4f156d58b19a656c904813c1b4a45a0029ae7f50731f8014":"f61b61a6e79a41
183e8ed6647899d2dc85cdaf5c3abf5c7f3bf37685946dc28f4923dc842f2d4326bd6ce0d50a84cb3ba869d72a36e2469
10eba6512ba36cd7ed3a5437c9245b00a344308c792b668b458d3c3e16dee2fbec41867da31084d46d8ec168de2148ef
64fc5b72069abf5a6ada1ead2b7146bb793ff1c9c3690fa56"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-256,256+128,0,256) #8
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"a459e1815cbca4514ec8094d5ab2414a557ba6fe10e613c345338
d0521e4bf9062221392e2552e76cd0d36df6e6068eb":"":"0a3642b02b23b3ef62c701a63401124022f5b896de86dab6e
6c7451497aa1dcc":"c80514865901371c45ba92d9f95d50bb7c9dd1768cb3dfbc45b968da94965c6e":"464e6977b8ad
aef307c9623e41c357013249c9ffd77f405f3925cebb69f151ce8fbb6a277164002aee7858fc224f6499042aa1e6322dee
e9a5d133c31d640e12a7487c731ba03ad866a24675badb1d79220c40be689f79c2a0be93cb4dada3e0eac4ab140cb919
98b6f11953e68f2319b050c40f71c34de9905ae41b2de1c2f6"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-256,256+128,0,256) #9
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"252c2cad613e002478162861880979ee4e323025eebb6fb2e0aa9f
200e28e0a1d001bc9a8f2c8c242e4369df0c191989":"":"9bcfc61cb2bc000034bb3db980eb47c76fb5ecdd40553eff113

368d639b947fd":"8b0565c767c2610ee0014582e9fbecb96e173005b60e9581503a6dca5637a26e":"e96c15fe8a60692b0a7d67171e0195ff6e1c87aab844221e71700d1bbee75feea695f6a740c9760bbe0e812ecf4061d8f0955bc0195e18c4fd1516ebca50ba6a6db86881737dbab8321707675479b87611db6af2c97ea361a5484555ead454defb1a64335de964fc803d40f3a6f057893d2afc25725754f4f00abc51920743dc"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-256,256+128,0,256) #10
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"8be0ca6adc8b3870c9d69d6021bc1f1d8eb9e649073d35ee6c5aa0b7e56ad8a59d1265f7d51fdb65377f1e6edd6ae0e4":"":"da86167ac997c406bb7979f423986a84ec6614d6caa7afc10aff0699a9b2cf7f":"e4baa3c555950b53e2bfdba480cb4c94b59381bac1e33947e0c22e838a9534cf":"64384ecc4ea6b458efc227ca697eac5510092265520c0a0d8a0ccf9ed3ca9d58074671188c6a7ad16d0b050cdc072c125d7298d3a31d9f044a9ee40da0089a84fea28cc7f05f1716db952fad29a0e779635cb7a912a959be67be2f0a4170aace2981802e2ff6467e5b46f0ffbff3b42ba5935fd553c82482ac266acf1cd247d7"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-256,256+128,0,256) #11
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"d43a75b6adf26d60322284cb12ac38327792442aa8f040f60a2f331b33ac4a8f0682f8b091f811afacaacaec9b04d279":"":"7fd3b8f512940da7de5d80199d9a7b42670c04a945775a3dba869546cbb9bc65":"2575db20bc7aafc2a90a5dabab760db851d754777bc9f05616af1858b24ff3da":"0da7a8dc73c163014bf0841913d3067806456bbca6d5de92b85534c6545467313648d71ef17c923d090dc92cff8d4d1a9a2bb63e001dc2e8ab1a597999be3d6cf70ff63fee9985801395fbd4f4990430c4259fcae4fa1fcd73dc3187ccc102d04af7c07532885e5a226fc42809c48f22eecf4f6ab996ae4fcb144786957d9f41"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-256,256+128,0,256) #12
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"64352f236af5d32067a529a8fd05ba00a338c9de306371a0b00c36e610a48d18df99ed2c7608c870624b962a5dc68acd":"":"da416335e7aaf60cf3d06fb438735ce796aad09034f8969c8f8c3f81e32fef24":"a28c07c21a2297311adf172c19e83ca0a87731bdffb80548978d2d1cd82cf8a3":"132b9f25868729e3853d3c51f99a3b5fae6d4204bea70890daf62e042b776a526c8fb831b80a6d5d3f153237df1fd39b6fd9137963f5516d9cdd4e3f9195c46e9972c15d3edc6606e3368bde1594977fb88d0ca6e6f5f3d057ccadc7d7dab77dfc42658a1e972aa446b20d418286386a52dfc1c714d2ac548713268b0b709729"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-256,256+128,0,256) #13
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"282f4d2e05a2cd30e9087f5633089389449f04bac11df718c90bb351cd3653a590a7daf3c0de9ea286081efc4a684dfb":"":"2630b4ccc7271cc379cb580b0aaede3d3aa8c1c7ba002cf791f0752c3d739007":"c31d69de499f1017be44e3d4fa77ecebc6a9b9934749fcf136f267b29115d2cc":"c899094520e0197c37b91dd50778e20a5b950decfb308d39f1db709447ae48f6101d9abe63a783fbb830eec1d359a5f61a2013728966d349213ee96382614aa4135058a967627183810c6622a2158cababe3b8ab99169c89e362108bf5955b4ffc47440f87e4bad0d36bc738e737e072e64d8842e7619f1be0af1141f05afe2d"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-256,256+128,0,256) #14
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"13c752b9e745ce77bbc7c0dbda982313d3fe66f903e83ebd8dbe4ff0c11380e9f1a533095d6174164bd7c82532464ae7":"":"4f53db89b9ba7fc00767bc751fb8f3c103fe0f76acd6d5c7891

ab15b2b7cf67c":"582c2a7d34679088cca6bd28723c99aac07db46c332dc0153d1673256903b446":"6311f4c0c4cd1f8
6bd48349abb9eb930d4f63df5e5f7217d1d1b91a71d8a6938b0ad2b3e897bd7e3d8703db125fab30e03464fad41e5ddf
5bf9aeeb5161b244468cfb26a9d956931a5412c97d64188b0da1bd907819c686f39af82e91cfeef0cbffb5d1e229e383be
d26d06412988640706815a6e820796876f416653e464961"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-256,256+128,256,0) #0
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"5cacc68165a2e2ee20812f35ec73a79dbf30fd475476ac0c44fc617
4cdac2b556f885496c1e63af620becd9e71ecb824":"e72dd8590d4ed5295515c35ed6199e9d211b8f069b3058caa6670
b96ef1208d0":"":"":"f1012cf543f94533df27fedfbf58e5b79a3dc517a9c402bdbfc9a0c0f721f9d53faf4aafdc4b8f7a1b
580fcaa52338d4bd95f58966a243cdcd3f446ed4bc546d9f607b190dd69954450d16cd0e2d6437067d8b44d19a6af7a7
cfa8794e5fbd728e8fb2f2e8db5dd4ff1aa275f35886098e80ff844886060da8b1e7137846b23b"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-256,256+128,256,0) #1
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"8df013b4d103523073917ddf6a869793059e9943fc8654549e7ab
22f7c29f122da2625af2ddd4abcce3cf4fa4659d84e":"b571e66d7c338bc07b76ad3757bb2f9452bf7e07437ae8581ce7
bc7c3ac651a9":"":"":"b91cba4cc84fa25df8610b81b641402768a2097234932e37d590b1154cbd23f97452e310e291c
45146147f0da2d81761fe90fba64f94419c0f662b28c1ed94da487bb7e73eec798fbcf981b791d1be4f177a8907aa3c401
643a5b62b87b89d66b3a60e40d4a8e4e9d82af6d2700e6f535cdb51f75c321729103741030ccc3a56"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-256,256+128,256,0) #2
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"565b2b77937ba46536b0f693b3d5e4a8a24563f9ef1f676e8b5b2e
f17823832f4ef3064ec29f5b7f9686d75a23d170e3":"3b722433226c9dba745087270ab3af2c909425ba6d39f5ce46f07
256068319d9":"":"":"d144ee7f8363d128872f82c15663fe658413cd42651098e0a7c51a970de75287ec943f9061e902
280a5a9e183a7817a44222d198fbfab184881431b4adf35d3d1019da5a90b3696b2349c8fba15a56d0f9d010a88e3f9ee
edb67a69bcaa71281b41afa11af576b765e66858f0eb2e4ec4081609ec81da81df0a0eb06787340ea"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-256,256+128,256,0) #3
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"fc3832a91b1dcdcaa944f2d93cbceb85c267c491b7b59d017cde4a
dd79a836b6d5e76ce9eabafed06e33a913e395c5e0":"ffc5f6eefd51da64a0f67b5f0cf60d7ab43fc7836bca650022a0cee
57a43c148":"":"":"0e713c6cc9a4dbd4249201d12b7bf5c69c3e18eb504bf3252db2f43675e17d99b6a908400cea3040
11c2e54166dae1f20260008efe4e06a87e0ce525ca482bca223a902a14adcf2374a739a5dfeaf14cadd72efa4d55d15154
c974d9521535bcb70658c5b6c944020afb04a87b223b4b8e5d89821704a9985bb010405ba8f3d4"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-256,256+128,256,0) #4
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"8009eb2cb49fdf16403bcdfd4a9f952191062acb9cc111eca019f9
57fb9f4451355598866952394b1eddd85d59f81c9d":"09ff1d4b97d83b223d002e05f754be480d13ba968e5aac306d71
cc9fc49cc2dd":"":"":"9550903c2f02cf77c8f9c9a37041d0040ee1e3ef65ba1a1fbbcf44fb7a2172bd6b3aaabe850281c3
a1778277bacd09614dfefececac64338ae24a1bf150cbf9d9541173a82ecba08aa19b75abb779eb10efa4257d5252e8afc
ac414bc3bb5d3006b6f36fb9daea4c8c359ef6cdbeff27c1068571dd3c89dc87eda9190086888d"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-256,256+128,256,0) #5
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"a6e4c9a8bd6da23b9c2b10a7748fd08c4f782fadbac7ea501c17efd
c6f6087bdacdc47edf1d3b21d0aec7631abb6d7d5":"c16ee0908a5886dccf332fbc61de9ec7b7972d2c4c83c477409ce8
a15c623294":"":"":"a52f93ccb363e2bdf0903622c3caedb7cffd04b726052b8d455744c71b76dee1b71db9880dc3c218
50489cb29e412d7d80849cfa9151a151dcbf32a32b4a54cac01d3200200ed66a3a5e5c131a49655ffbf1a8824ff7f26569
0dffb4054df46a707b9213924c631c5bce379944c856c4f7846e281ac89c64fad3a49909dfb92b"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-256,256+128,256,0) #6
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"59d6307460a9bdd392dfc0904973991d585696010a71e52d590a
5039b4849fa434a0aafb95917cbf8c38fc5548373c05":"0407b7c57bc11361747c3d67526c36e228028a5d0b145d66ab
9a2fe4b07507a0":"":"":"299aba0661315211b09d2861855d0b4b125ab24649461341af6abd903ed6f025223b3299f21
26fcad44c675166d800619cf49540946b121389894179043 24b0ddad121327211a297f11259c9c34ce4c70c322a65367
5f78d385e4e2443f8058d141195e17e0bd1b9d44bf3e48c376e6eb44ef020b11cf03eb141c46ecb43cf3d"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-256,256+128,256,0) #7
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"9ae3506aadbc8358696ba1ba17e876e1157b7048235921503d36d
9211b4303429abf7d66afee5d2b811cba358bbc527d":"0d645f6238e9ceb038e4af9772426ca110c5be052f8673b8b5a
65c4e53d2f519":"":"":"5f032c7fec6320fe423b6f38085cbad59d826085afe915247b3d546c4c6b174554dd4877c0d67
1de9554b505393a44e71f209b70f991ac8aa6e08f983fff2a4c817b0cd26c12b2c929378506489a75b2025b358cb5d040
0821e7e252ac6376cd94a40c911a7ed8b6087e3de5fa39fa6b314c3ba1c593b864ce4ff281a97c325b"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-256,256+128,256,0) #8
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"96ae3b8775b36da2a29b889ad878941f43c7d51295d47440cd0e3
c49991931091fe022a6fc0237b055d4d6a7036b18d5":"1e40e97362d0a823d3964c26b81ab53825c56446c526168901
1886f19b08e5c2":"":"":"e707cd14b06ce1e6dbcceaedbf08d88891b03f44ad6a797bd12fdeb557d0151df9346a028dec
004844ca46adec3051dafb345895fa9f4604d8a13c8ff66ae093fa63c4d9c0816d55a0066d31e8404c841e87b6b2c7b5a
e9d7afb6840c2f7b441bf2d3d8bd3f40349c1c014347c1979213c76103e0bece26ad7720601eff42275"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-256,256+128,256,0) #9
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"33f5120396336e51ee3b0b619b5f873db05ca57cda86aeae2964f5
1480d149926f1f6e9807ba5393edcf3cb4e4bb6113":"3709605af44d90196867c927512aa8ba31837063337b4879408
d91a05c8efa9f":"":"":"8b8291126ded9acef12516025c99ccce225d844308b584b872c903c7bc6467599a1cead003dc4
c70f6d519f5b51ce0da57f53da90dbe8f666a1a1dde297727fee2d44cebd1301fc1ca75956a3fcae0d374e0df6009b668f
d21638d2b733e6902d22d5bfb4af1b455975e08eef0ebe4dc87705801e7776583c8de11672729f723"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-256,256+128,256,0) #10
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"ad300b799005f290fee7f930eebce158b98fb6cb449987fe433f955
456b3530006aa2514e4bd114edf7ac105cfef2772":"87ada711465e4169da2a74c931afb9b5a5b190d07b7af342aa9957
0401c3ee8a":"":"":"80d7c606ff49415a3a92ba1f2943235c01339c8f9cd0b0511fbfdf3ef23c42ffff008524193faaa4b7f

2f2eb0cfa221d9df89bd373fe4e158ec06fad3ecf1eb48b8239b0bb826ee69d773883a3e8edac66254610ff70b6609836860e39ea1f3bfa04596fee1f2baca6cebb244774c6c3eb4af1f02899eba8f4188f91776de16f"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-256,256+128,256,0) #11
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"130b044e2c15ab89375e54b72e7baae6d4cad734b013a090f4df057e634f6ff065fd6ac602cd44107d705dbc066e52b6":"f374aba16f34d54aae5e494505b67d3818ef1c08ea24967a76876d4361379aec":"":"":"5d179534fb0dba3526993ed8e27ec9f915183d967336bb24352c67f4ab5d7935d3168e57008da851515efbaecb69904b6d899d3bfa6e9805659aef2942c4903875b8fcbc0d1d24d1c075f0ff667c1fc240d8b410dff582fa71fa30878955ce2ed786ef32ef852706e62439b69921f26e84e0f54f62b938f04905f05fcd7c2204"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-256,256+128,256,0) #12
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"716430e999964b35459c17921fe5f60e09bd9ab234cb8f4ba4932bec4a60a1d59533b711e061b07d505da707cafbca03":"372ae616d1a1fc45c5aecad0939c49b9e01c93bfb40c835eebd837af747f079d":"":"":"a80d6a1b2d0ce01fe0d26e70fb73da20d45841cf01bfbd50b90d2751a46114c0e758cb787d281a0a9cf62f5c8ce2ee7ca74fefff330efe74926acca6d6f0646e4e3c1a1e52fce1d57b88beda4a5815896f25f38a652cc240deb582921c8b1d03a1da966dd04c2e7eee274df2cd1837096b9f7a0d89a82434076bc30173229a60"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-256,256+128,256,0) #13
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"7679f154296e6d580854826539003a82d1c54e2e062c619d00da6c6ac820789b55d12941b0896462e7d888e5322a99a3":"ba4d1ed696f58ef64596c76cee87cc1ca83069a79e7982b9a06f9d62f4209faf":"":"":"10dc7cd2bb68c2c28f76d1b04ae2aa287071e04c3b688e1986b05cc1209f691daa55868ebb05b633c75a40a32b49663185fe5bb8f906008347ef51590530948b87613920014802e5864e0758f012e1eae31f0c4c031ef823aecfb2f8a73aaa946fc507037f9050b277bdeaa023123f9d22da1606e82cb7e56de34bf009eccb46"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-256,256+128,256,0) #14
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"8ca4a964e1ff68753db86753d09222e09b888b500be46f2a3830afa9172a1d6da59394e0af764e2f21cf751f623ffa6c":"eb8164b3bf6c1750a8de8528af16cffdf400856d82260acd5958894a98afeed5":"":"":"fc5701b508f0264f4fdb88414768e1afb0a5b445400dcfdeddd0eba67b4fea8c056d79a69fd050759fb3d626b29adb8438326fd583f1ba0475ce7707bd294ab01743d077605866425b1cbd0f6c7bba972b30fbe9fce0a719b044fcc1394354895a9f8304a2b5101909808ddfdf66df6237142b6566588e4e1e8949b90c27fc1f"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-256,256+128,256,256) #0
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"5d3286bc53a258a53ba781e2c4dcd79a790e43bbe0e89fb3eed39086be34174bc5422294b7318952ace7055ab7570abf":"2dba094d008e150d51c4135bb2f03dcde9cbf3468a12908a1b025c120c985b9d":"793a7ef8f6f0482beac542bb785c10f8b7b406a4de92667ab168ecc2cf7573c6":"2238cdb4e23d629fe0c2a83dd8d5144ce1a6229ef41dabe2a99ff722e510b530":"d04678198ae7e1aeb435b45291458ffde0891560748b43330eaf866b5a6385e74c6fa5a5a44bdb284d436e98d244018d6acedcdfa2e9f499d8089e4db86ae89a6ab2d19cb705e2f048f97fb597f04106a1fa6a1416ad3d859118e079a0c319eb95686f4cbcce3b5101c7a0b010ef029c4ef6d06cdfac97efb9773891688c37cf"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-256,256+128,256,256) #1
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"c2a566a9a1817b15c5c3b778177ac87c24e797be0a845f11c2fe399dd37732f2cb1894eb2b97b3c56e628329516f86ec":"13ce4d8dd2db9796f94156c8e8f0769b0aa1c82c1323b61536603bca37c9ee29":"413dd83fe56835abd478cb9693d67635901c40239a266462d3133b83e49c820b":"d5c4a71f9d6d95a1bedf0bd2247c277d1f84a4e57a4a8825b82a2d097de63ef1":"b3a3698d777699a0dd9fa3f0a9fa57832d3cefac5df24437c6d73a0fe41040f1729038aef1e926352ea59de120bfb7b073183a34106efed6278ff8ad844ba0448115dfddf3319a82de6bb11d80bd871a9acd35c73645e1270fb9fe4fa88ec0e465409ea0cba809fe2f45e04943a2e396bbb7dd2f4e0795303524cc9cc5ea54a1"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-256,256+128,256,256) #2
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"a33288a96f41dd54b945e060c8bd0c094f1e28267cc1dcbba52063c1a9d54c4d36918c977e1a7276a2bb475591c367b7":"6aa528c940962638dc2201738850fd1fe6f5d0eb9f687ff1af39d9c7b36830d9":"37ee633a635e43af59abdb1762c7ea45bfe060ec1d9077ecd2a43a658673f3c7":"2eb96f2e28fa9f674bb03ade703b8f791ee5356e2ee85c7ed5bda96325256c61":"db2f91932767eb846961ce5321c7003431870508e8c6f8d432ca1f9cee5cdc1aed6e0f133d317eb6990c4b3b0a360cdfb5b43a6e712bd46bca04c414868fab22c6a49c4b89c812697c3a7fbfc8ddf10c8aa5ebf13a09fd114eb2a02a07f69786f3ce7fd30231f22779bc8db103b13fa546dbc45a89a86275281172761683d384"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-256,256+128,256,256) #3
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"5f37b6e47e1776e735adc03d4b999879477ff4a206231924033d94c0114f911b7d12d62c79c9f6234ae0314156947459":"92d4d9fab5f8bf5119f2663a9df7334f50dcde74fb9d7732f7eba56501e60d54":"c9aef0d7a9ba7345d08b6d5b5ce5645c7495b8685e6b93846ffcf470f5abd40d":"50d9d1f5074f7d9f1a24a9c63aa47b94da5ba78db1b0f18e4d4fe45c6875813c":"20d942bbd7d98700faa37e94d53bf74f2d6bd1d8c95c0b88d842c4857797d59e7c8788aeeac29740122f208f703bf35dc32b0035db0648384feb6aa17a3274bc09b2d2b746c5a06fd82f4469fb86131a49482cb7be7d9b4b95042394cfb18b13f333ec0fe5c227bf1d8f33ecb2e42e358b6c3e034cb585331bd1d27f638029b9"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-256,256+128,256,256)
#4
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"2311c5afd64c584484b2729e84db80c0b4063fe9ca7edc83350488d7e67264a06a6dfd975a0dc7b72df1f107c4b3b3a6":"2abd870ec5fe26ed14dfa57a3309f920131b70580c3639af2645cd1af93db1b1":"c6e532a3b25653b6002aed5269cc2118749306e736bde039d4d569d4f967773f":"5e7d26c4da769c373092b2b4f72b109fe34bdb7d169ea38f78ebae5df4a15759":"cacaeb1b4ac2305d8714eb50cbe1c67c5a2c0bbc7938fdfdcafef7c85fc40becbf777a4cfb6f14c6eee320943a493d2b0a744a6eb3c256ee9a3763037437df9adce3e2260f0c35e958af0edb5a81debd8bdaf2b8bb2b98b9186e5a222a21609ff58df4cbe1d4898d10d6e7c46f31f5cb1041bfd83a5fb27d5c56c961e91403fc"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-256,256+128,256,256) #5
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"362ece9d330e1172a8f9e50258476d0c79c3ee50346524ba12d970ee3a6ef8c5cf11bcb4d9d51311ceacfca8705e833f":"abb5a8edde02e526449284ecc31bc713383df3ed085f752e3b6a32f305861eed":"746302ab1f4a86b17546bea762e929360f2e95c7788a63545a264ef997c8c65e":"b907c5b2a8833a48e

56e819228ce9a050b41b3309f5ca37bed720311d92b33af":"73c7131a558350590053580873ef956ff952f2aa6ff1bea4
52e013d1bc2afddea2311756dbe756e63ba6258480c48f3f6c1319b5f572f67ca530af09e39413d1d432bea8f89206619
618cb0e7c88e9f2033639d0eb0efc20616b64f940da99b88231984c3fb23f19e890576f555fde394dbd4351f17a7ffd5c3
69379001bda03"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-256,256+128,256,256) #6
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"cf614bc29946bc0095f415e8bdeda10aab05392f9cc9187a86ea6e
c95ee422e177fb5ec22dc0432cc13f4693e2e3bd9a":"e4ce77914ffbc5fddf1fb51edfafdc196109139b84c741354135ec
8d314c7c43":"e1e83ee1205acaf6164dc287aec08e5b32789e5be818078db39e53cad589db51":"4e20c0226d5e1e7e80
5679f03f72452b5bea2d0ba41e0c12329bf60eb3016dd1":"838fdf1418a746aa52ae4005d90c3fd301f648c5770ffef2a9
f3912e37a93850cc4b8bfcce910aead0cb75958823b1a62e283901c5e4a3980e4ea36257458e2e4953555819b8852a26
489b1d74821f80c9908469b43f124ff7ea62497c36159a47353098a1b9ec32e54800d6704371cc37f357ad74aacc203e9
b6db97f94d0c4"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-256,256+128,256,256) #7
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"a8da1d3e233f393fd44d204c200202f7d01896e72c5ac652940cfd
15b5d4b0bd0a112b4cb0890af0a495e0f49fcf6874":"d2e32799bc822b8d033299bdf63dc35774f7649e935d25be5b10
512c430d1bda":"920a82d76fcd2cd106ada64bba232b7b2344f3afe6b1d1d20ee8795144571009":"eeaac58782753720
25f8231febed64db6a11273c3c00d625fc80a95f18ad7d3f":"5f6dae489b53d89027b2cc333c700f090152d77b3eaf01d
47f56ce6eca9893ef877b4cb560fab0fbdb34e3d1c6cd8480b33c053d2661a10aa531df4961b97d659c7492584236582b
3fe701055efa59c328194cd1e07fcffd910d9ee01b7b9e8c8fda7f7ac01a8e203b8b26eb8078a9b9a5021562c44af24089
e3ef84c1d5a6bd"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-256,256+128,256,256) #8
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"a77b1ed4ecaa650374e1052c405f1d88881c25c87d13dbe1334d8
c1a847fa76b05c143e2f145db216fe7be9ed23635d0":"b5c750968ff09ed251d4a1c05342ac843db5246b19045728a63
4fa4f6e752e54":"ff5937bcd01a363696bf8e40adc8e4ab3e56dbf7e7d09451c99e538785fe6697":"4acb34eea8266badc
f8f6557a0eecf3eb4d7a295c876d6175598cb66a388efb8":"ec13eadfcc84e77d2a2efa1a2cd8b1355587cb27feb3d19d7
5b37f0446333ddb8236e751c63b7a6e595ec24a25051a696dbe8c062dd8896d1446db228a2f10e8094ee07e7ee648ed6
bebb2f5ec5aae24c9c640665c28355cc11c116795ecc070790f7fdfc4398900311b6695d5da0175091ed1828d2731085
bfb4a20bd86cce0"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-256,256+128,256,256) #9
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"491686c781e83eb4e21d9989e8d718100b0d21a2c56295888baef
1a65f219651499085296d21065feabf3106101c8d6f":"d208a72f9ae34f0817669fb04f49239dd31700f3dc9a93db8d75
fb79f9b686c1":"9ffc61893a293a864008fdd56d3292600d9e2ec8a1ea8f34ac5931e968905a23":"4ff3a397dfdae09120
32a302a5e7a07dceca8d9013a21545689319b7c024cd07":"3c258ebf2203fca3b322ad1b016e21c7f5c148425f81e4fb0
a0e462dce9dfa569c37a006527768297a5b68461b08912642a341b88c85597e30e7561206886098c4e2d861f11513f0f
fdbbc78d3a2dd60c105abbb33c5e05ae27081b690fb8b3610917aa9bf1a4ad74481b5ff8334f14e5ad6a6a1eb22594760
78076fb7e3a992"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-256,256+128,256,256) #10
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"36a5267eeeb5a1a7d46de0f8f9281f73cd9611f01198fdaa78c5315205e5a177b66b5337970df36219321badacc624eb":"c2a7b164949da102bece44a423197682ff97627d1fe9654266b8527f64e5b386":"a977e2d8637b019c74063d163bb25387dc56f4eb40e502cefc5ae6ad26a6abdc":"c5c9819557b1e7d8a86fa8c60be42993edc3ef539c13d9a51fb64b0de06e145e":"b471711a4fc7ab7247e65d2c2fe49a50169187187b7978cd2fdb0f8318be3ec55fc68ed4577ad9b42cbb57100b5d35ac86c244c4c93a5b28c1a11c2dfe905d608ec7804dec5bb15cf8d79695534d5e13a6a7e18a887ec9cf184da0cbbc6267f3a952a769403bafcdbb559401be0d8b3300ea7258b4026fc892175efd55ba1a67"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-256,256+128,256,256) #11
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"a76b0366df89e4073a6b6b9c04da1d6817ce26f1c4825cad4097bdf4d7b9445e773d3cc3290176773847869be528d1a4":"1bfd3bcfb9287a5ad055d1b2b8615fa81c94ac24bc1c219a0f8de58789e0404a":"edd879fa56f21d93029da875b683ce50f6fdc4c0da41da051d000eed2afefefa":"f528ffd29160039260133ed9654589ce60e39e7f667c34f82cda65ddcf5fff14":"39d1ff8848e74dd2cdc6b818ad69823878062116fdf1679942f892c7e191be1c4b6ea268ecdff001b22af0d510f30c2c25b90fc34927f46e3f45d36b0e1848b3a5d54c36c7c65ee7287d325dfbb51b56a438feb6650ce13df88bf06b87ac4a35d2a199ea888629fb0d83f82f0ea160dc79ed220d8ef195b9e80c542f60c2d320"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-256,256+128,256,256) #12
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"46571e1df43e5e141235e2a9ec85bb0faf1dc0566031e14d41a2fbd0315653ecb60ef6a3347967519aabeaf748e4e991":"759fd8593e3688b23c4a003b655311770d670789878570eb3b155a8e6c2d8c45":"033128460b449e1accb0e9c54508759ddc2538bc64b51e6277553f0c60a02723":"a5e4a717240bdeac18a0c0e231a11dc04a47d7550f342fa9a7a5ff334eb9327d":"9d222df1d530ea7f8f2297a0c79d637da570b48042ecddded75956bba0f0e70b271ffa3c9a53bada6ee1b8a4203c22bfde82a5e2eb1b150f54c6483458569422c1a34a8997d42cc09750167a78bf52a0bd158397af9f83caabe689185c099bf0a9a4853dd3cf8b8e89efebb6a27dba873e65e9927741b22968f2875789b44e01"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-256,256+128,256,256) #13
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"d63980e63bbe4ac08d2ac5646bf085b82c75995e3fdfc23bb9cc734cd85ca7d2d33ed1dcae13fb634ba08272d6697590":"acd0da070072a5340c4f5f4395568e1a36374e074196ae87f3692ee40487e1df":"f567677b5e12e26f3544be3da9314c88fc475bf84804a89a51f12b191392c02b":"c01cc7873e93c86e2bfb8fc984cfc2eab5cc58eeef018fedb5cba5aedd386156":"b133446f633bcb40724bbf9fa187c39a44b9c094a0a0d40e98977e5466dc2c9adf62a5f4551eeb6406a14658de8a0ed7487c3bf6277e811101284a941745ce16176acc875f1435e14161772fa84609e8123c53dd03cbb868030835c0d11d8d6aa04a1b6f908248b028997737f54735ec4ed7a81fc868199ffb61a779d9340334"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-256,256+128,256,256) #14
depends_on:MBEDTLS_SHA256_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA256:"3d99f9b7ac3a2fbe9cf15d960bf41f5588fc4db1e0d2a5c9c0fe9059f03593fb411f504bb63a9b3afa7ffa1357bb48be":"0bb5ebd55981a25ba69164da49fa92f2871fd3fc65eb30d0f0d0b8d798a4f8f2":"288e948a551284eb3cb23e26299955c2fb8f063c132a92683c1615ecaed80f30":"d975b22f79e34acf5db2

5a2a167ef60a10682dd9964e15533d75f7fa9efc5dcb":"ee8d707eea9bc7080d58768c8c64a991606bb808600cafab834db8bc884f866941b4a7eb8d0334d876c0f1151bccc7ce8970593dad0c1809075ce6dbca54c4d4667227331eeac97f83ccb76901762f153c5e8562a8ccf12c8a1f2f480ec6f1975ac097a49770219107d4edea54fb5ee23a8403874929d073d7ef0526a647011a"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,0,0) #0
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"a1dc2dfeda4f3a1124e0e75ebfbe5f98cac11018221dda3fdcf8f9125d68447abae5ea27166540515268a493a96b5187":"":"":"":"228293e59b1e4545a4ff9f232616fc5108a1128debd0f7c20ace837ca105cbf24c0dac1f9847dafd0d0500721ffad3c684a992d110a549a264d14a8911c50be8cd6a7e8fac783ad95b24f64fd8cc4c8b649eac2b15b363e30df79541a6b8a1caac238949b46643694c85e1d5fcbcd9aaae6260acee660b8a79bea48e079ceb6a5eaf4993a82c3f1b758d7c53e3094eeac63dc255be6dcdcc2b51e5ca45d2b20684a5a8fa5806b96f8461ebf51bc515a7dd8c5475c0e70f2fd0faf7869a99ab6c"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,0,0) #1
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"067fa0e25d71ea392671c24f38ef782ab3587a7b3c77ea756f7bd496b445b7a3ce6acc722768ca0e03784b2217bc60e4":"":"":"":"16eaa49510ffad8cc21ec32858640a0d6f34cb03e8649022aa5c3f566b44e8ace7c3b056cf2a44b242de09ae21dba4275418933611875841b4f0944a8272848c5dc1aad685935e12511d5ee27e9162d4bb968afab53c4b338269c1c77da9d78617911ed4390cb20e88bf30b74fda66fe05df5537a759061d3ffd9231d811e8b34213f22ab0b0ddafff7749a40243a901c310776e09d2e529806d4d6f0655178953c16707519c3c19b9aaa0d09fb676a9d23525c8bc388053bfccfbc368e3eb04"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-384,256+128,0,0) #2
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"9f76503e84727297bc7056c7af917a1c98baa725295457db4fcf54ed09af7f15f39c46142b85a67b4b323594b7e97bde":"":"":"":"7d6a8bc5a7f057ceed6109bfac2486f80f81373b6b31d062aa1fad6d9eda5874867b9ef007ba5a92ba8f3fca624bfd9f7ee5770bbeb0391394fef783c16a7f003c06e5469bab03445bb28a2111def415d162e40472d3e5ae628c5c63170bb19f741c79a5331c883c12bca429f518bf71b14683a071b6c6e1e55d8c7a0f3942bc12a103556c49ca173e498b3b4a15027145cdaeb195bc8a7e1aa82ebdf6ecd516481a4d21f400d0d71b5894545888fee8beed80d3251647947f5abc4735b47fd0"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,0,0) #3
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"e242e5b3b49d87289fe02840dc742a2a6cd9490fe2cce581833dddb1edc0d103f987f5de5c68cd345c81b032ea55f36d":"":"":"":"3a858345dfaf00defdf6c83114b760ef53b131fbf14bcc4052cd948820eee78a11cbbd8f4baa308e1d187fced74cbf019c1080d9efffd93fda07df051433876d9900c1f9ad36ea1cb04989bb0c55fd6d01e46923f3bc8887ac00ebd4710212114165355361e240b04232df55a81add3fb363f0d4c9c5e3d313bc7caac7d49dca8517cedacf571fde9686ae93d901fb9b17097a638bb9899cfab0ebc9d1f8a43c2eed7c9f326a711d0f5b9cfc5166c9b561824cbd7775ec601ca712b3ddaaa05b"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,0,0) #4
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"42cc17365f5ea5fd22bdc4ade715e293064d6794d82bed5b77c4c

107a73de1f76d759e4b191ba01e0ed5dea788ab018d":"":"":"":"de06dee8c8fe453aa03ac2546c39f5cda12412864d52e
d5cbd0d4905dd226746d50d1af9fd3e1d90de0f16295cb7f6f4d3271ef00564709df4b05eb9f8adc0f8e8522b05b9f32c3
7d8526813898b9f71db57fc8328e3b79144482e8aa55c83934d6e097e43ec6d0bc32edaf8c0e6ca449b2e8388b32b286
e2d4f85266b0605fb99d1a647565c95ff7857bcab73662b7218719189d792514edca2b1d0cdcd9b6347e132ef4c323da
24ad5afd5ed6f96d27b0f879288e962fa0baca3d5b72b5c70"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-384,256+128,0,0) #5
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"d57024a230b825b241c206f7b55e2114461ecc9b75353f12ac1d9
ad7e7871481fe401c320f74afdb07f566ea500b0628":"":"":"":"e8930bd55a0a5a6d83a9b3b2cde7085c2ae467ea4a2e6
5ca303697d492ca878bcb801769eb1b7ec564586ec8b36d350e192c4fbf03a98be0ddecf56d465914ba353ed7734d19a
680fc4593d9234c4ac8c23b7dfa1e26b013f590cca43b9fef126121b4842496b11dea3ef5e981cb357341f03f92a546a62
609236ded6f7d814456acc0596d555cbdc02cbd47dae2caa1897831ea464225922c6600a8bb92e711653067f83b21e1d
f054309858948c11a1399736fc8391c5b0fc35629abfa5650"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,0,0) #6
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"059ded79125b2d56d9d52bcc950bf608d1a2373515dafcc81efb6
588005a5722d8f5f4181f9f2a316c93fdfbadf50e75":"":"":"":"db65d2000632c3d7009c227e99c210e5897f4d7edae60
8a242b5a4f17708613f8c19a4dd65d6bc3ca57737c9bfdcca068288eea49440af768d1fc977c32b065bb71aa3d8c4d77c
9e8e8a6166f332a247978a6c41ed253a1b68ad934a3416b40344a681de28638f00b0a0ffb75514c3f62253372f8099060
43de35e4805b8e962e5eb957f04212835f802b2c0b3e76c7cf239c89adf31909cd6224d542d929f9b20a10ab99a7c631e
4e6188fe2ba8f552c9c88fdadb528679fe950431641b8f37"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-384,256+128,0,0) #7
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"4630406b475b1263b6078e93e5d4282205958d94eb97d1e66b42
9fb69ec9fccd0dd9982c338df935e929c42fab66adaf":"":"":"":"5d80ec072f550981bcaac6787c0488cc470406249ec80
f4bf11050630227f8b5ac6b3b369db237d7c24a0980dffe8d3abd9b64fd4efa492349bd4eb6902edb94553546110227d7
de5a864ddae8b9fed8de9f0df9c596e39de903fda323ee6f788831452eb9e49c5eef3e058b5bf84f61f735a93e042bb9e4
58df6b25f42a6eb8fb03d437cfab757fab4990c721a757eaa5e9048208abbcce6e52f177b20dcf52f1fa551a92b68bcdb0
1680855b8f79131266378cd1f0c2a4141c9675f01d1e48"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,0,0) #8
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"6ea9c6f784f12a9707ceac8a7162ee5381dc893ee139f8f4b4d93d
b266829db4ae92bc52ff860d8ecdc9fc16bd070130":"":"":"":"234366f1591cfe244956f9496cdf446e0d390ba64beaa0
66945b1b4c5337dded2619dd2bd0133a5d612bab7c251ab79e3951cb134894c422553fc8cc7b3ccb29c20adbf52dda35
af779142d7efc735342db2ee067649fda25f3e8a74f8e4f6620cf5a17cb943602609cafb85bdf482873efa4c74928cc0d69
444b72aa6bc72694a3a21c6a721aa4e0fccab0a98aef375a37a3e8a15dccad13b6d70b3483581004642d879804aa00cba
207b51affca43490bb98f67953265574366ec3829e67aa"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,0,0) #9
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"5c13056be92a7f71236fcfef460298acc8595dd474310727f5ccb9

a7acb2254ac7226f86349e20e2aca737068ab0f2ce":"":"":"":"16d415eddefa4dc295a64adcbbcb8c6fe8c8f123c6b09dc
08a56d723cff5978cc120fd0a68a2f4c202c220db372d3128ef52385d5786c12dfc6e60ecfc3461a09fa80453e2b1b6365
eaeb4df602d192aacb25ab6b4a59689d4bf8d1c4c42a32779f62b06baca6461f154cf40901f5787c1aa2bf67cbfe7546ef
5b2bdff20790d8c72d077d48c59c92d1af90a90ccfcdf643dd9d6cee0b1faf5f2f35cfd01d2077ced5e2d013ec1e09336df
ab9d9e51ba9a3a2837306213bca2d79abf8dc3282c"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-384,256+128,0,0) #10
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"38f08a099fc2d405c32d1e0f867e5450d5ee0d53783c31de9ddeae
46d962999da01f13a43320c715612cedb920cf12eb":"":"":"":"079ce7a5b540cae96c2883e95acde3039048a6c45a2d2
59cc648639e7205392d91fa3ee080e615f1e0741a0e536c9e05844651b93461bfc547fb452fec61f853e1bd6e08eabd0cf
1c5f84f85eca9d42b53d1e5bae51be5fd35189e4f1c02b843c6361fccf4ca6648bf30a23ccb8ebc16fcf158746eb39cd96f
19d46707c001e11c4e0e8ccbc89fec66c69fc92843b6bb2ee1cc7595b65ba89ccaccd6130a8417faf705e8e203e90ee64a
e970c409389b5cd0ca80a4e40b642689741691b20621"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,0,0) #11
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"0863c868c32442a1a64095a71ab6ae2f9e61c119b58dfa4f34efd2
6593bbbf68bc407904c43300452dd4e61df47fa98f":"":"":"":"585334828cf531828fc7127fee0c926f85b8e71e8522ea
921296dc62b83a09a00397cd45e0664d0f26fa24edd3e3d8ecef8fdd77ab22431d4066f0efaf3882c97f179a7060efe9e8
cba5d8145bebd502c0e09ee791231d539983c08860d7783edb58440d193ed82bc77c27723381a0da45bb1fc2a609f8b7
3b90446e39869a5af5038aff603b44db9771113927a5297fdc3450eaa228e313afe43c31b0a95b476c5ca312b4f589f80
9749481722cea9990c02b647976aa6c6f02ce1e5e6ea6df"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,0,0) #12
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"a41ad223e41e2bb9c131ec945ca310600ab00c51f6e4fcddd803bd
9ab9be8af5483373838894d32745a81ba9d6967751":"":"":"":"95ca31a7eeebdd2348cf1d43411d2c35faffdbcaed4052
d50cf92f0e9d2e757686b72d631a56ca98b68215e7014cfed943abc1e13441c1d660f13adf2188d0975154e1b42a592a6
2a43b57f82cc21a428873a92fda83abe420efb5233140e4d6c7852cf81e85961fa5c606c5f33e06077f414b0f814cbbe50
cc606bffbd474364e608825fdaaf5e74d862795539be8697e2ce05d71446881e3f65bb54ed95e941586988f6e0c34e1be
ef426696e9dbd9a214013d826a8c99a2a686d8402c583f"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-384,256+128,0,0) #13
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"62a26c1327c0ebf8b40691fb4c8f812e81f5474b0c7db70aa94241
10fee3a05e41c0cf2e87210e34d0c6bffc269bf2ba":"":"":"":"6e20a00df1af37e6cc55e580ba21335111eb37539534361
8df7d630b9dc234496e3964cd45c5de34bda46a28964f6148704c30925feeaecae0574038434cd33c1dd943207a8dbdc
d72dc9ecb76a25728b3c2a8ac13c1de3a126d7d43a46e12e0d0ca8991469e582b78ef6aa691b5a0e3e85cba7d7aea3c1e
8e031674e85f5af36546eb2a0a28d4ffbaa316a9a6c944fce291cc0c235e8499882eb62b22b548ae07cf9430329e009f44
43cb94f7a14e8661166b0d681dcec867205abed48145e9"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,0,0) #14
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"fd54cf77ed35022a3fd0dec88e58a207c8c069250066481388f128

41d38ad98591f9c02a1d205cdbcdf4d93054fde5f5":"":"":"":"f6d5bf594f44a1c7c9954ae498fe993f67f4e67ef4e34950
9719b7fd597311f2c123889203d90f147a242cfa863c691dc74cfe7027de25860c67d8ecd06bcd22dfec34f6b6c838e5aa
b34d89624378fb5598b9f30add2e10bdc439dcb1535878cec90a7cf7251675ccfb9ee37932b1a07cd9b523c07eff45a5e
14d888be830c5ab06dcd5032278bf9627ff20dbec322e84038bac3b46229425e954283c4e061383ffe9b0558c59b1ece2
a167a4ee27dd59afeeb16b38fbdb3c415f34b1c83a75"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-384,256+128,0,256) #0
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"5e919d353357671566d2c6ab6e1acd46f47d0c878fe36114d7fea9
fecb88a3a27efca9e3d1e1b09d7f16832f3af75141":"":"442f17cb3cb1482a19729bfd58f46f6ef16285554892c01b0718
968d6e011082":"f9557c93eb841bfd7b5d4b71da928efcbe3f55e1870493ef90d16eb238380d65":"36902134f1989cfe
7eb518a56c06aada98997d9bacd04aee21f879a57b515ca3b5e0c2d5fed05ca1a8b054e8c46b389d9d9186feb0abe8e2e
60b3a267281cc5b4b7341116ced35a0e07bc2b0330bbfd8b07f07248fa6d8fc5c9df13445324162bdfa22a91ba71453ab
123c92f91c70b8bd540b3b180b11ab45ae2c59e57c7c43dab7576594959a96eb502d182267c86576b1846ccee1a694ca
bdfb42e0c8214192efb502926fa3c27eed020b7cc8866a5af9d838a57e78bf7acd230e1f4d8361"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,0,256) #1
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"7a5d1efc9b7043060cabd67de7fe22740bcd6a8ceb355d69f11882
9a2b3c92006a5633e613f8769c1114b1822ffb5408":"":"f2ad962d992434468681c644587639901ff74e2bbdd8761961
ec34edc4a0c36d":"75aae0d1bca9484c89fc4de3d1b34275ef0656775f3f8c96f2bbc50401aaa718":"5ca21af4b399db3
8f8b74a406aace69f994691f2765bb9c47b240000152739e059b163cd007de5f28bba17e485fcf9ff6f41f76e93998510e
302282cbdbde09fe8b1a96187e57c9a3df94e2e748f20026476ca682dfa890b478f7a21f4927f74f99aedd9ae782ba10fc
da1dc34c31b4f784722e01cc4679737276f56df23c5bd8c6985797b83c0ccde2b4c7a65c652745de7fc8a235ad7ed0f45
6f1e7568b2dad475f0bc46f02a7f35c05cfef9d0e2c773ff895e291a2cfc2424b106096d8864"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,0,256) #2
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"611586ee40cb3ca4a9238ce112a237449bba5422ac9b18ea53480
875334d8fa026da9d96c4e87f94b2f9a7c261be3edb":"":"2f835c336a3aa0019b0bf940c24643bc8fca58c9cfa6509aa9
241de9e0e1a046":"1911a59c5f2568860ae71e803688889dc44d14ffb0d93e324c39f32d95c1c3ea":"27bf42f50476d8a
2cc23f455e9ef477cb8e9c90f2e97c8a483093ebf55b2aee02e0356cff919e2ec9811b42c73498a6c2b96aa5b761ef7e71
5cbf66ad2e3ff8a6c92419dbf2e653ce70a87b51e26d9f607eb25b45b91f947d0026a38977143c8bbd94076e663b9cee3
5505b48e453e7cca83e540975ae8a53f26390aa63aaf1e2669410cc83427eea09428776a2d520eebd170602c52dd491c
98042018a0372a0b39cb565cbe5e474f927f91515a6a7444fdbe1d89d8ae2c2482a0deb8ff236d"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,0,256) #3
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"85b1e5da599efd4a20ffcefd4737fa3ea1d2b14be33861c2a4ac3ac
2a49d3947b14cf18f4ff426cb6345f1a7653e9630":"":"cf5bbf98d8577077b0b84475dee0f0e9aa95eedd1d916507b523
3b688bcc856c":"b333ec111e1e7d78c9ac916e420704832539d2db46aca3bdc4732e8ce72b5e80":"4773d32a9fba37ac
c6900f3ac70f6978ff1e40039d6e3286c264fb7fc59f1bfe0188c7979380c8922bdd0e363c8e09a49faef59ea85a9f0e400
b94c74a8a50687e4e51e25266eabb86276f22628d0d2e19c5696cd221a9b80f94045d001ca4c20dc916ca0ff22c93a41f
c822912dd7e247927fd45982e94d3d1fde77cbe78beecba830b753079326ae33274f13fb7cd875e85fb5e9e703e61cbd4
1bc4ad47d7b4d14afc873a39dd810ad8eed95adff8dce3adb7659b7c1d4e3f62403767940b4"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-384,256+128,0,256) #4
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"50f986f6efb413fba3e8e0beb84d4948c2db0661ab8e064d9fee8b3c2f0a910fc35d37512f88bdfcfde797a21a006e01":"":"37c7b08222ba63f2136bb28f5ec09b9a899b56371615be41bef49a0b640590e4":"4a1e34a5d60ca08e3e6c0f1b86547ba2d12fa293275e7d75f83a0b846daa48df":"e27738c6fae66125fcaf4e725a0881d5a450fb5b02a55057d6cb7babd91d502c4f4a8431a83352f47ea8e5fd7e815f5080d144318a1dcbc755e0b935785cd5397955da22e3ff633b34a64ac72b2e6b7c51e78ff553731e6e8da911d147a6e05b36b74898cac6d3171bc8650e445ffd19ede2aa8218be17671321c186465d852dd80d73290546b88ef7a978b41c4c549e9c7fc6ef86e47084778fb5aed5d41e794ee0e700b77c0314a307b10df69daba605f3fdbe2dec708ba0b20d6b650befbd"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,0,256) #5
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"641dbcbf99b61437c2bf65a13dc3e0324eb940335da123870d9429636dfc82979d0cc913c73e8a6321fc3eb9e973c0aa":"":"72580c11a87ce6b4207908aaf5bcaaa1bd217fce3e8bc0726568c64639b70767":"cf9f4527e074b72be735558dcaa1fc82f26ae286bf944b49649f769bf6faf49f":"345395723d048c2270c0eac990498689bcb862a4996e82995b4e7169e671eb03bb2242c4669c874c1aeaffec58aa653c7d7431abd1650f0cbce8cf5db8316693f3ed501fd9b48c1a44b34f7878aa386d65afc31f94f908a322b03d06c2a1074a03bd2b579cafb0f7cee6d6934588ae1ce9e4ed37b03737c553ca19af4b46b5e43767cee2e459ab91407df6cfd13a6f186abdb148b85a5f49bf92ac6674fb055c7fe123e9355a0d33de281c03a56f91891dd496dabfd6eaa6fff6c9cfb4e67c44"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,0,256) #6
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"b9c305ada943a64a2b00494e869f9a640173eb1c2518dd9be93abc3c93c7e6b5bd0627a199d15f77b188824df00d5997":"":"ffc6760f9af02d35666275c074eda03f53dbcb5690580bb25768a6566b328dfb":"f26f436a820ef71597b75134b8d9dca6e9a6afd9b429222a4c9c878f3b92716e":"e5413a234859511cd837312bb31aac4d31962c5f7f27aec47417f367ca99b8400a4287e60412fc356cb40d96ddf5cb801285ebca42b2f6fe4a711451c1574174c58dccb2cd3342b7092a196ac7d2881a08e7f5de939ccc8f4eedc8f867c81aa88655d96ae50f618279d5009ba2ac4b1df4e63030cc0ec3541b6a94bd9a2ae5d1fcf4d847114a783c997a7c6b9d549010bf7b649abef692cdea3aa8ada14574e0f78b7fcbe17b587ac14980e40264d6de030e429586593d5ce3ae571f95454dcf"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,0,256) #7
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"9875dbf59b760eab9998bf3341847910526d10071dc179f96081dd793a6001936881e7f39075cd382293a1aaa8c845d2":"":"1196583a99afe1d377b344585c8252a0690704b8f7a2b7582387ec91a60fd7e4":"20147a88e0f9f1e8caa8cb14488c9b5c38e5520a36ae913b4703d15af27218dd":"c808f6f296683d26208359a766fe61bc70ee8b6ed9ffb94ce269578fb5568fe2358d603638324b63b29bb36ae71a542e38ee69a2b93ad7e4a887a27a2852cdcd541a5fa6d0c8b087aa1185bd5788256e7d95c2aa2d5c11407b7bf762f416b01d8e747c45298f875200a2e67679d6d5ff7a7c0e50a010690b1920df1baf0afcfaee7ab0862004e23b5aa1ff47b8273d503bd74a54e7b39ac7e6d6fb0a594d30531cab8a67b22783470a65f24faba1c231b3ba45efae9f0be04e2338529cfec008"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-384,256+128,0,256) #8
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"ac92a6c791aba0406d6ea8255c3c0901eb711a424501c2c2c847076d78bdcfc3266b7c3bc578c7501daac6dda8366d4f":"":"13379a77d84a0c4cec95e62ac4c8a98ceede0d89b8bd31735

2a95300963415ed":"04d47ec89a3e1b7f22580167331225a00ff258da72446241a6c09c517ee4d48c":"c2e6528584c6d
bec436ffec4075fd3aebe953fdc0b46b4b225a3c2886e60d21879e6ccce3746d881f6d80e33876afad439ab9f68fcc4584
92de12811fbd57ac49d868754da19279b4c0a38979201a588884def5677392dec97cafc94bccf8914d9f78575711bb6f2
adf4116db91c8b54e36e9ac2f5e01caebd300acd7bd45eada69d20f1b4139013a8a614069315a1c99137a6f23e38f91c2
10e0c156c6fb498056e823dc41a05348ab43c2f6f4ce188d4e05a13d38f8025731ac1670949a040"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,0,256) #9
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"63954ac7a0f989a458d2b4a6b7013dd66683624584b545060bd0
3a57b92822ef422764bbbc35fa5d40d34145afe44bec":"":"7b25d875dfb03333cc27b9d4286d00a85ea5921f4b8a4717
b957349eb3509053":"8b70d28c5c80086c0cbbd01337ad45297af271d4bafc764b0fc5705700cd419d":"297752e61c4
ebc4e1c68391335e2cdb49b0f19dafe359e451f8158fb7958d32a98455a852002d8f05169f438816ae6fccba1eae4d1fdd
7a1176b04831d7ce892f711ec825062ea1c6b12144bbd3a0aca7f92520ebb87ac6045d2ac3a4a74fa559926f0daceb59d
44fdb39f5fc3b877f34241531e863c153286f3f1b2ba2db4e2c8e2344be40c2a7a8cd01daf168696ce19f83ddb64d50e23
13e78c5dfcf077f25e5b4d6f687279119ce856d4131a63ad133cedd020881939bf70f82eabfe46db"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,0,256) #10
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"d0944e0a3f3604a588271c8eb65913ad9b07ee2b29620f8106ca7
0ec10aeb896bc9b2b519c77fec5fc419e953ceb0be5":"":"d58593f2488f0a292ab552dac006c94b20ff500dd57af32be8
08921a5ee251c1":"ea9e579c9dca67f07ffd67d2483ec1fac3d2ec22fefff73c7ac9f125888d7a4b":"ae736da6632a7d8bd
cc9e279cb7d3f9101a8f7dddeff253277d1d99b45c76a1a5c193334e912c3dfdff1bc389b209c3b29359a4ca53765a1e40
cb900c6055d8a285cf63ebec79b46019efe95d5199f215f11961f3319d225bf3d60734fbfbf3593ab105cec2a17e308af4
69b3220ef7f055675396d289e6f4f8009881c8a2b4e9de88d53ad13e8bed8b38be6d8988f615b4590fde3d91caf50a86e
ac3fbf29924743145803978d261132b5975a9f108499250314e098e57c56e2f9327307cff8"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,0,256) #11
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"1ef53464bc7a441227a27ea7b5c558dbb3f509aaf880213cdef7e8f
6a1d287c173cd5b3148d46c48c83c5cad3ccc1f50":"":"b052a66992fd8a8cb02c593edfe4766fcbcd3505af29d698e1f4
db398acf717d":"37333448311c2c6edee19aadb8f1036cb60cff2a945c1a0ea087713bff31e915":"4ea7054659cae1cc1
78ef431aebb64c2c8dda3a965ea940a84c00d9790e2e3a33521395cc4d49038994aa4c7dcaf0b52b44375d93b625ac22
81991a85a5acebf3de552355e17b3528faf39d392fed981400f28540f5ca64a4d2eeb952c88856c8f7388a49611810941
b46b1000ee4a8aaaadcd39944c4abca9110fd6580093f9303f86a6e129d56b5aeff5422c2261af33523cc6a174e0782e13
a026c003c17430b8371bbfc3d51c3e06fbdc30769a278b109238bbe383cd5523053fe589b72e"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-384,256+128,0,256) #12
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"14148d69d583d4c1758c307e0eb0b762511165823fc54096f9da5
513e87df53b96a7be8d31b8a38f24a82d846b0e13ef":"":"e05f81f6402c52dff5c221a2f191155bb56abe160ce7dc8a6b
edfa029195a612":"214777e3faee7d953b5c796675e106d50cdc12836b3114d14447ae91cea3c1db":"eb0497b32af8a9
1ed3959c31b079b8cc5c39db3100913332fffbb6b1d5ebbcdc97d6e67c934f3336197c9b730d80995a7d7445e36cf304
7cab22895f244cac803eabd001eb1ff5d5645a803c41ea6dde6c972b47de0372ce901667d03e2e02aa0a5aea809e0bdc7
430440365908418ce6066c24191ace05d6a797ef9b94409989cacbb9d9ec31f3cf0112b72e1420b47e0c184a8aacc214d
55a0d5e0869d09303e4014de0430c07380006ea75984e6c32b06067d7d7b931e2b74666b4b569f71"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,0,256) #13
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"27d47020acc3a80a55149fa0ef43f684843ba89fda4bff1c29d20baa2b21956780569b7fa0c4078d9ff71a3790f1be3f":"":"c03ea0b88e2f9b53f902b22746bf4dde09439c190a7a638e3cb990d86739dbed":"3ef05e71487cdbc209b5ab6e808e55f0a93bcc02df766b01c1c1ae5875b1023e":"3ee49e2a58d800d922cfb66284da84bbb5944c85f194d95f1156b673392132a430e47ae74f1ed7c1d0e632d8cb604c88777437d8f37e7d0428b834555a96800540bf5bce6f430328fd328baf4b22b7f8e663c1d8583bc0119248588840510e11203cf47dfc4f6cdf8344170a341fbb7d93999ba86be3fb94d9c03922fd3d75e3fd5b42365aa62606e352676b2a0c51fb030d8d5605e8ac6bac2b4f8417d8e060148e3d4ba67b31e5e704d866bc87741ba877d12b10e8a9b37f3feca908fe1fc4"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,0,256) #14
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"88b6550d49182ca7321d8015f780121223a93343dabaf21978ee2818e7bce6591d32b48eb4642069adcaa5986224e6d3":"":"809639f48ebf6756a530e1b6aad2036082b07b13ed3c13e80dc2b6ea56e70a04":"3395902e0004e584123bb6926f89954a5d03cc13c3c3e3b70fd0cbe975c339a7":"4a5a29bf725c8240ae6558641a6b8f2e584db031ef158124c4d1041fe56988fdaee91ca13925fee6d5e5748b26cc0275d45ef35abb56ad12e65aa6fe1d28a198f5aa7938fca4794c1a35f9a60a37c7360baf860efd20398c72a36b3c4805c67a185e2f099f034b80d04008c54d6a6e7ec727b1cace12e0119c171a02515ab18ea3d0a3463622dd88027b40567be96e5c301469b47d83f5a2056d1dc9341e0de101d6d5f1b78c61cc4a6bfd6f9184ebde7a97ccf53d393f26fd2afcae5ebedb7e"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,256,0) #0
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"2cd968bacda2bc314d2fb41fe43354fb761134eb19eec60431e2f36755b85126e3dedf2af9382a1e652143e952212d39":"59fa8235108821accbd3c14eaf76856d6a07f43383db4cc6038040b18810d53c":"":"":"06051ce6b2f1c34378e08caf8fe836201ff7ec2db8fc5a2519add2524d90470194b247af3a34a673298e57070b256f59fd098632768e2d55137d6c17b1a53fe45d6ed0e31d49e64820db145014e2f038b69b7220e042a8efc98985706ab9635451230a128aee801d4e3718ff59511c3f3ff1b20f109774a8ddc1fadf41afcc13d40096d997948857a894d0ef8b3235c3213ba85c50c2f3d61b0d104eccfcf36c35fe5e49e7602cb1533de12f0bec613a0ed9633821957e5b7cb32f60b7c02fa4"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-384,256+128,256,0) #1
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"023f5673dac29f62245510d0a866629c43c64bf35a0bad30f1270050876cfb1ce80b615a5a47ecb51217a46079e11fd3":"a6f797b155d6da01f5d155cb7291442e1b82d4190e93e279fe5b4aaa7d04ecc0":"":"":"507b824443af5db28f746229e03ab00c73cc3ee4956aa14b33eda00dd2b9b645c132dab7dcdbc659c8ba0e1a3575fe7dbc7cf9691f9b714acb1b33bef96943003c992f661e04fe9e8b9f648f4af9a58a45b08b8fa7fa3704e6bdc289abbe14a8c7e1747a52ac916c31ed079de0b900672e658a201279824d0d75ae35dbdd43aeab915653765d83e46f347fcb4fe3321fc28abd2d0d26a662661582ce21b6dc4ea6d1b236e9692a83c8ba0fb299157b80623ad4f448d25d57f537b10e5e30f80b"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,256,0) #2
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"96b5bc16ce0d101b90d54da6c4b3d85a70ee19d54cf4cde3d048af

b5f758a6b52ea2c10c16feb71cedfab9bfa9e462f8":"2ff415e2432d2e6c4279910a5e56c0f5354a5af0099132d891943b4a8901ca6c":"":"":"ecebe717afe6dc08dbff3ed626bb06de0f9784283b70e378dec19d4fbb50e61b7be48ceb69851b2bb94641aec5027d53d314a96500a9bbb38a87c9aa42ebeb96a23cf29a0fbd5e48b399daa1b24dbdc85223f24b7d77332bb1a137ec709d27c008c709696cbe44bb2fc19fb10a2fad4ffd8a9d89492a939f2268d1557f44b6a64e2a57887830fd8bca1b6306aaedbd7f3f476b827995a1ed121388497edc7e639c87d092f6591a45b5647c6c091c15ed39f594b7fc4ae92331f96dd8e17be970"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,256,0) #3
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"364a833a283a3e0b8a5b681daa50df96d806d4b54828f2b016de5d88597e6287d98cba8fda464d21aa1cfb7b26b9b226":"35b0e7534014dc2d7eb0f20ff78a69d5548d0a64122d4936a6ed177fb3ec66a6":"":"":"df4c799cae37173a81c545d019ffa336ef2c039a5865af425e5b60bc3d7202f4bc1aac5a84022bf4088061abd5c39d0fb047ba80163eb5dc8b9dd515948f16915832c6f76b45acc25b9c01e7f70955c0eb51bf50f00b24bb8e7ff53bd7c051b53d8b1a837a17a00355d7eb21e43b2b5b249dadced37d06e7047c2fd12012705a59d051afd26245ce3a59acb4b996b718c7dc1ae964bf12b1db02fd6c06ac2fec6ee5deb02c2c830110e9bbbd3c778a136b646ce2a0738563555a89409c56b81e"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-384,256+128,256,0) #4
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"bb4d38c775acdeed663256abb747ec25182bc16efd0de02cb4b05e4ad4749c92be6f1e856e423a8f3bfb0c0f27ad8210":"21591e796b7e68e7913fefbef4872af9c062f21c8023c0dbf47e040c3aed3733":"":"":"12575776e1b9f54b0fbc39e85a77b6912160bace4f1e9f049e3a1c5bcb452cf9be42ea10c028c3cc249401ac236dd3baa53ff327735435f4869d3289bc9465ccf15f826e4e4fff099986bdde0d09bd12e3caddcf452eed6ca1206ae4561b84770a9cc6e962567304ef79d8d3608529a3b5e4067fa83c8c35a06f1855da5f5ea7eb106e4c60181d12ba00cfbf7eac60bda00571d95c45c9d75c43b42e27a238aa5e0f02bbd96cde59a2e572934a99d05c399ffdf15c65f173748734c51999a29e"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,256,0) #5
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"f9d041d24158f480600c3747cbfd868c3f7e9ac7f74b3760eae5320839e4f5130f8477d88b1d914c0d8b375d089a4c83":"b148049f4093f0032c7f105dae219aa9e3f70487ce3a6b6ecd99429f66be5406":"":"":"84c58bf473061da92fa8d56aab3a75598428f18dca504191a51746eb5fcad8f784eafac5ea81d636d579e330baf7db95c8d706432e9f585e84da090c0eb40dcd819bf10e0d5b8600150d186f732af50b431c596c920eca742e6555129fdf5df96b44005083d7a33087b150d63529bee4b6e1ed4189ae2d93cee8dc671d47c0e74ba04218dfe273484a4bb59a57743ea56843d516ff2c72ef9841996d31b0d6c5beef367a6b44cc84cf4d403a06b40406e4c9f47da401e3cf31412694e6164dcb"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,256,0) #6
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"c18f511ffc3479a59357c17c2fb3d1e0e6f0edda4c8b567f2413323c2037f2fd140fb0cf33eb59526d8c0dbd216939b5":"7387aa3b0b3d92afb29761d3d5ea16e32a68297b9ea6751e1d54c8612f6351c1":"":"":"949bf03868563c7d1498c69c327686682656374b2efdef6342e69a388229c580ca2217a9332d3ae77c2d1223f5dedf4b34ec50b79d5baa7283168ed7cbe71c6c3c9193bbe01b76e011c39d2d462017c2c74b7e698fa2140e16886a9ec0fc6c36decbae37537638ccf17777f1cfa49d2c2c7ba3aadd0a1565d61942de94aa6fa16ecafc2dafabc9082f23e75a0e2f8f79d1c0a15ce57fef7655f1a4fc6fc4d4a694bf6ca9e333959f35ad354524f614905c6a52ef8f524cdf01c5fa

dadf207772"

HMAC_DRBG NIST CAVS 14.3
No Reseed (SHA-384,256+128,256,0) #7
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"6b09295110384eb56726f61474bdc532fdace31ceadb5fc23d5873
56cfac74338ab6f9d89394b907edb646650865a3fc":"7cafcb4db31ab411c396015b8bbbc990607e08bd1cef3337dfa0e
295ae024f9e":"":"":"e51bc5b3a6bb2a2667f5d62c2ff9902dd07b566870b4c14242627da7581449ec985739cdc2bb5ef
036033fa798112ce20df06d46d61aad7121b8282fe7556bdd363cdabbf47184e55edd85ee0b7b0be17b9a7f822f4d8906
465b525c16385d0899b6c27728ff2a600870aef65f58f9d3777e8987d86e59fdb69cd232e7289fc75cf2174304137f988
a17b60c57af84cd8e556aaad458f511fc0b3009516435c0c60098f35fb6a4a90d90bc6071d38000703ef57cbc19d6b78a
0f797f3ba044c9"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-384,256+128,256,0) #8
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"ec6d0f68240f5c47e822d9088364c6cd03ca53808162b4f06f5956
da65290946f4d26653d079e50604f836c1d798243d":"b40b5737cc76c5f6d1df0f13bfbac7e26f92aa933125705b6197
d9bedb11f2e1":"":"":"207833cf65599e1406ddaf3452f060c872099cbf7483f1f7f14033490f7258ca5fd7f5339f914498
b6e61fa426cb872c880a9fda9b8ba590cd8006b990af7ad412f60c8b2ad969c2f9cb0e9d005943d4dd2dd7af9699046ce
89d6405597716d43b9ad54641c2278b04b2bcc5b8ecbcd5e2044e4e6ec5a628605fcbd67249e813bb769d7df01b6040
4d030e69e9672b4fdeddf82a22042b83ca036578b69f9a0ad9702bcf95fe846705b49b0a0795dfbc4f671e0158ded6242
bd8f8fbc2410c46"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,256,0) #9
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"df59ac224e4ba1b6dff348f17bcf9c5a94a3235a54f2799a6cae29d
8654b79d18b09b444a28a7d537e1a2bc89e95abd8":"14a0a91e0cfd63ef5fcbe2e8c7a44bcf5769c9f95b6c50bbe9d3b4
8b82a09053":"":"":"656438e7738d441b9ac116361e9f26adc0e303da7889cf559841b3e44127318edd356051bd0b3ec
ea78feb2b928227921a0c183c9f56bfd11ef31b28da6c78f3891d8ae1804bc158fa56e8b7a1a46be4954de493ef65a7f9b
eb46949a323a04e944034db30b19cebd8b70bfc155882ddfaca1bd5acb981c2c1b3e0862c6234d13093ddbcdff15129d
586fc24ea2fd20946fe45b467bbbc77a6b6973eb6ea02994607c657eec29e4c4b3915cb730db056babf1779127047b40
1e25f97f606063b"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,256,0) #10
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"8da1ad6810c1d6b7ead210e48f51c370d4520547a330a4d591e61
a9847aa043463f69d1b237999fda9b5697f1e7aaa07":"291c536dac72409e31e71cafb1b5f55c14421b2c7a44d792cfdc
663dc8f62692":"":"":"c2bff571554c26bbd4442fbb3b0f8eb4db09840337658a7425613e0fd4f96e60da39b250c3a773
79a53325a56ec02248c4d67fb9154e3b0eb8972a3109aed531eccc027705b267d2b9c037da79860d76e5e980b5b30b7e
a588fa221d24d973f6d4c625de65123e91613a1528cdee59993aa827f319a759412f20aad6c50fa79a3debeb346ad9280
9470daf228cf344e09f03c839a28d580a2b3d7050685ef51e95649aba7228a2f0c82a2dfd89cae6ce549e8b27fd46f02fe
b473645765018ef"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-384,256+128,256,0) #11
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"5e8d6571f514519de6c4c0a7cc5b85df616735b8dd09c3bed2377

499aaabb296a9b2c94642da10e8fa737cdfb3129334":"6ae29c71b76fc48f14a3d731a0f6f276f73e7672eff631dbb1d22b06463bb236":"":"":"5cadc1264314fb4bc7ed7fa74bfa16aefa624bf2fd60c992d0cba10429c56e0028ebb430b1a1c6662a9b3c7f6de244ca000ae63db9570f1aa3e7ffb1e97a9d848021d8e632fedc037712a29abec4063b9d57c60738f0af0b1aab3844b03f7aacc65d38bec91a11b7c3bf8d970f01e00fed9dbbe9e2e499a21c72a7c5a22864125133ecb073a4c9f6d9fd46024f5c1ee7fa447209afa6ccef1f97ae77ca67fca5959dde209d2597f87af6e154408579cec42c69fa9b7cc075ee3e37ee3d91ad9f"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,256,0) #12
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"5c9481b2642855fac8931eccd1bd6c5a05b560a55f96d37e865f057a95812d81fe65c84c96a990eb7a302b58de723cb4":"b6a61b9a31207363d62c0b88f1632290f4f18feb41a6dedb85b7450ff9157016":"":"":"9cc77b68e1ac23fdd2e2a6ff697053f816bb48b39b1162f7aa3fdd2dd1867f68b13980c9e5989d4631b7983248501731326bd7bf6e967b3dee7d2d5625d3cc2e198623af9f77f86103491ebb4aefda5c333b51557b8f643e6d6c593fd7e27e4bccca13140f6129cbd024de076e4688567fd7e41dc7b2bd0bd9b3e966d5d3c461502221b52b001a4d2102894da04172efb900171a0eabab1fd134217580cfc33a0a94edc0bc132af91d048c6f5ea4e34ebc9686a99f81d19118ba4da63ae3df7a"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,256,0) #13
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"c43f883d0adc2b56984d4a497a8ad76813a01df5a0ba22b53144763b65c7bf3f6f722e4ceac59966a6e44ed898e6109b":"769bace2c263edb87101743673724ef67a935e1ae9cace87202b6015d20fd9ca":"":"":"ce61480953190453247d091838dd80117f7f85a7e9a1237c92edf10cfa26b423735788b1e89f33625480d9faae57112ee62c8e4840475a6a738018ad3fd4a77efdd8f15ffb621c429419b6adb20431fd35f9d62fb33d500b87beac4856aa4971eb89710576b609ecfe758f3682dd316e7ee9d6560b444c2446656c8941dca7d6eaa70fdf8a70f18386ee5d4c86738bc261c0e8e5f509dabffd0425a86858ea3c71de5be98570dabd80a37b4f7f954002727c0b712e58693603c23130a45e98df"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-384,256+128,256,0) #14
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"d083f7f8c65374627ddb51582b3a39e2bf074508d5f28ecce25787f386058de8afafaf2ad7e6449308e176be01edbc59":"ddb4ced192f52bdfa17aa82391f57142ac50e77f428fa191e298c23899611aad":"":"":"b978826b890ce8a264bf1ad1c486aaf5a80aa407428c0201dd047fa1b26e9ea9ff25a9149215b04c2f32b65e007e0059a8efe11481926925061c748678835c0066f596352123f0b883e0c6ab027da2486244da5e6033953af9e41eec02f15bebdb4e1215d964905e67c9e3945ec8177b8c4869efc70a165719b8e1f153c41744d44d3c56a15822d522e69bd277c0c0435fa93e5e1bc49bc9d02aee058a01a04580a6cad821e9f85cf764fc70dfae494cbfa924eab0eff7842e3541bc29156f6b"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,256,256) #0
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"c2feb900032f2cca98d3f60536f563d8ac9af5fb2e90dba36c371c0a1c58cf5e4a60f2be0fa13b8266b715be8aad128c":"8e6f9be0c692648072d19c750804b10e2ec313c8013abd363de7a467787859f2":"72f54ba3f8e71ad69a040bb8493283acfc8815f17dbcea220ecd68372a2dffae":"adce8157ef60482841dd2ac5ac512bf7649120c1dba81ea75f2a70b7512bb6f3":"e76e4326ac69ddbc6b2408c529b05a96425c65cc65671601191238e9434d2a0147f3a25ce9b6818774f5263c92459bca421d2b492f9a9c2971359baaa1426d6e2c36d8924f39d02ee2fb5502c4e0b206dbe9aeeacd508abe6c055d547b5f9f35de4fdc9c05a2c63ad699a3a7e265598b8f40a8a295d7376b88c4

9af9edc790b8a5ee221e19877616678e2a5135d7b3756109200439d9ec8bfe0cc5f3c334ca9c022ab9192d5d554dc7ae76af1dc06d814427f46a7cfa2dcc62f4777d07ebde7d"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,256,256) #1
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"ad500edbe28b9a4338b55451b81c652797eb48fba753c186ce0aa9ad02a84ea2c995b7ade6de0fb4ec97bcbd61b711d5":"5770c41832a4cdc4039a8c332a4b45e7a7b2dabb678ccd2e56452aabeab14925":"d8d5516d158b41cb9d66566b88064900af78183f765f2f72a19548fb797377b2":"60a3a01a72e6b3f33a0c236db08237e7d656bdf4bab1db57ae23b7305569dea5":"c5ac3df66bc664e8bf84c758c7926992f0e8a03cd3f3f5fb8277c85b4da526601e8131f9d205f35594e101a86fb83ccf4c1e98c8e609062256701ff2132e337cb7287f0ee2e8fe3ef11ae703d7efe52e63cf89119ced05950c55aae6c822b6b0a8e1b91b537e5bb2de165a4b5b43a1c41fbfd65fff9bc5329d303caca84f5d1fc6acacee622623ed5dde36aeda0816749557c924d6ed26cd80e456fd0ae2146477ccb63a203fe16ac1d0eb2d12b6a2cabb21d412422e95f2df8ccdc23b4ef0dc"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,256,256) #2
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"51a29bac53961792077e88ed3603d33bd1f51b3fdb2b5cd1ea131c6f643af65de81eb2e260396d2a69b4184c4eb98a15":"72e5285b92c4ea4458e8a2159687cd46e7df9c1f4513d8b72cc88be41c2e1522":"16a69f7aee34c567595f3d362ccbdbb7b9e9372c4b1729fbb80d9a089eee31a4":"825197262a43f6523182f0a91005d70b17d81c2bb692edfd02ab988130c7d5b9":"f63f531c242a295d7796c3b4844fc74821af5a53e0e7ae822cd8a7f9de91e6164164f3448fd7d18feafb97c9500e0625d501dcb3927e6fb39ef65dd9586d157076436452bd3066cb30d1f47dc0a3ffa5f2e9ab4e183018b40a82b39b0d170aa21b05600eefea906838b95456e04cf046808030a56951d2502c5eb6271228905ed08549bb171d6c0408d88250785f42e349ce1d9e74a6cd0360a008ec804e7ecdcb4d1fe24aa5a18cbb65f4de1619a29c6062b409a386ea6f43e60adb9ea3dd28"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-384,256+128,256,256) #3
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"b30ff9c6e5b6bd258f1cea0fd5ef9adb81fbec233ff2fab01e79b7422878b2e950604e10ab80ddceb9d2b968d0d37ba9":"e8acd4b380aace0b27572057eaa947e10e6b49516140139c74a1d4f472221dac":"1d2ded0003521e2ba6a4a3e732e0949c1d858fdf0925fedd9cfd7f603e0e692a":"688ac5e7b4400d962c106fd2ce712a1cda6a0b8ac5196ad727f9b882329a3d5a":"c5208fec1d67517311a42bec07782ceb247e9c818e4f5f3bd160c9e53d462b61884feb278cdc8f64e22f59d27dfa98d3a90da8c7c5ba28ca40bd0d18934595a376553d1a8a19de07a83e2e9db42748c982cbcbf4a975c20084ea9cc6c6a41b571faf66b364e4b7e4d32efc80c30b219da1c02a1ea02f6922adbc31a057f999605a2d827f10907835c2bdde4157d7bf2906a0ad27bb72f113c6ec4f23631a2b8517bbce91b560d90d73fbf0699bab21da23e27cfec513bb5e375f50108197d664"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,256,256) #4
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"56715dcbaa4f5bdbd157bdd950d1c1b46c1f4f8d7818ab321d72c0ff3c0a928064b0439f7bf021dcdc7febf2126e5432":"cd5547991b525f7795e075a59af1701375175bd760db99d316b91463f87f7f3c":"b2e4f02f1c14866f538eddab402356ff3b405abbb9154e88b98483a83be70f7c":"b8db321ab30285eee7f9e377ad62def6caada447d00a4ec882081daafe2ec009":"7ed8c2be58e3553eb65508377d63d7f24518d1a7235dd4c740bd987dd8bc1c1e3ca97a69a37dc9a270ad88989e4868e6cf8e4cf01703c0b1eb6aed8c3f8af431d819e68b6947ae134d360d87e33668cdef0e45e11f5cd79329ff95ed00e4a6952750f1574f489394b5fde3c6f07311a1e5d9c4e070a0943ef9d4a130a9e4b0a80c256e96ca5042961766874898ea0f772b78d1a33e866351a4eb425b822b5ad596cf249bce8ccd6dafb

334b71a503fce2c8fa3fbac9943910ce5ff02ebbedde8"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,256,256) #5
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"1c60a31760019e6a571e2987e57e19adbc1accf3edd44e501061cb
ec331b197eb68d0fa8fa5e3071d6f8b7c9c0a3c35d":"d4d84dc7311096791dd9c9d7f2cd291071f877afd86b96444274
82d09ac9df64":"6473f4430398d7e5a2d218bd05e6aedac1e317269df3e4705d56c22d6e7abb0f":"379649b56a46399b
9ab5f3880e1a73993a58cf52821d3cac87890aa0e6322a94":"d34152fa12fa341d0326a525aa83855863001385774 7f0
2634d24e9deec2da12f52fb405e7f1b973dc2d982d26eb2ddb4b49c35a9308b06809171dc990a4248e6da0c329a259f4
95247b9fa8c73af06604db7b629168e34081696a043977dd29a3c0362d5895f9aac24bcba58dd74078ef6f8d33eac864f
2e6cdc479da3d224bad8099d011e914b6ccc3631a7369586e18c71a4087de0d47a7c29a09c12438c7de2d4b47768f476
85b742c25b860e716c31e2afe4ce6d92bc2fb9f34400602f9"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,256,256) #6
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"eeccce7f7edc52f0e2559250be36526cd1839151a77c59d527f66f
a24ea4d86b3fb298c8d72b6a0a8e191b60259d1fc1":"26d35895723ba3d431991a0e6fb2154ae5bff7e58609c926ee32
69afc5cd631f":"227b9a71a6c17ecbf627161fc627f8f6f1a28ce39772b7a3d36064e2cc6dc4d5":"eb59f780c5a955e135
5dfe15cc4a4e90a6ec75584e63bd0de734399f47b95070":"78ac77657dc56b23e617a9b38168da945c1cf52b6062c2b1
0f1d7a3814d9b9efa5545da050b0db5a65a2d2d2e02fa12e97eb970fa8e83c524bc809d675e0db35c9762323f327f1edb
9b534ce16d02519750b41ebe51f747e9da43fd1afc60e46c7aba72e15cc7a22fad19ed55189f287a14737483eb6b32d96
6c3e3969d8198f01f2ed841f20d7d2e156d6285a29e07f6d7fff42bd575806c4092522b03e0d1b8df0cc88f5b82d24a7fd
0feff6ada03a60ef2541a4ab041a49aa973c7163bf94"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,256,256) #7
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"86f8104a081c9565dea5652f20145a068dadff125debf818262d89
31cec6ba937fd5b51affcebee952fb67f29f197267":"c7ba5ff828855e6e78fa1732d63aac1f49701ff7ac1f3506e97941f9
98b4e9d2":"6917bca15db53a5359e5c4d30ab4d37fc6a1bc660faaf2e74864cb4aa52e0e02":"eea8db0cfc04f8de14d60
53442b5b4f8733f822df4be5966a0de8b0f7d2036f6":"562b8b2fa3bb15cfc3f7e57f309e31b13c790c928ad6b32a005f5
431c28576c5706c4ac0dc2c7a4435bebfa06571278f485932bd94382efcf727b300b230da9b9e9f377d2659ac75dd8247
351d5ed8185effa0f255a2a2136e63717e0265d561a34c75ecee1c774c25e33fd938696825686acf9a419c1da3fa1ce8f6
95e231087aa0927dde6ab487dc61291ad4700c5c608fab1a418f6b30ff97b8b8f01ef8164287849a77b21be5d11d82d0c
19056e07d59a30f6c576705c6cedcb9f22d3a8f"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,256,256) #8
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"0db6f73ab6d31ddf8f78d76961310d68f081c9e6d5985e1883978
c2dec48d9f58875ab658b3a8b795bf464af9470a90c":"d886936ad36549a10b5dc5d6e21203abd75ad63f826794b4ada
ad45a70424c5f":"76993d3bcc32546430efa30e3b30acc34c7672b6e18c7e2e9a1f1cc26f7f7a22":"54c72cf3457e6f5f6
b35dc14167fee9383c44c867f233ec9d81f187bce438c0f":"c3523894d273c85d605d39f5b89e3388afad8c20787897b9
03d8db7e3de7590340174be3abd7598daba7806ab934e0feca02bbe66282d469ec01476bad5ccba59fc14cd9549bf4af4
9641f4326b1052b179c89194d21bec0501c97ef2c24aaf045fd348b765910fe92c0039612e37baad2445b57d9db6c1e5
50adf6688a79b117f6b7a37e0209d89f194a1bfe1ff2e3b28f0454b383af8872f32322bd5313a3c9ca48d33eab7c3807bb

98f8f402c43b99b2176f0b33be08c7e84c86b26e971ab"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-384,256+128,256,256) #9
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"3b1ffbfae6ec54a175a80a33c8768fb60f2af9ee2b8620c4e800a17fb9241ae47f77da414f67b5d7b24dd100355d2afb":"0d50cf61e2020a909ba6e36ba4d0a394579d3e4377cd4bf0068967e8d0fe7a78":"5d4efb3f6e6503c5d85a1c43398d0441ce8aefafaabe2f6d86988a24e033f502":"cfb6156a1b139abf21c73001240997ee1a8cad91a4bd777c0372c1e8fcfd3fac":"d3ef776c8d77fcc5e947bf53e0be11777e69c7dce138f24c1a3212d1b6b932580371479b7619fc82f029d92969628f810b54a8fdab8eba799e750945f3545f6a96226bc760ad736101516efff5d8581f5864b38c29885d39843a4adca17046e1e388c890542988797b576da64804eb4101638328d3f8bfa398ffaf83cb7290a2cfd39ead13290ae773a8958b33914ca02c8ff6a069aa25ac8b36f6f0f1dcd8f1c5fc838083a64ae7ae11b85be3a9fa80ed83949b622002e91776273fa32d6cfd"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,256,256) #10
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"19767ce1f18aea366539642fad400a03a675b2f3c0b1cfd49925e535b2c2779043c5a1c57ef550acae733729516aa62e":"6bfa882c1e895eeffbb85578182653c022a4703091529780c075cd482809b990":"11236df1dca3de6e3e3a57d2741d1b77f15f45b05beb47cc500100b31188a42d":"98708a88fafae56c4f6fa780c6c0e33ca8f2592983b5ae607146cd6e92204416":"b6514a3779dcef2c9ea0ed7ddfa808d045c5907314c358302ca32b2055987a38ef601637cdcf77b1b8f7eac479f8f18972013c2e1a6dfe612e8a586dc529ece486505534c0ff3dc0b2049a0e46d7ac504a1fdfaa9b08d9fa017c5803415fa391ba7eeb576fd6ddba4404feb46e7cde56e090dd280be5edba7d6df9c5ba7d3454bcbd4d443b08fb51a117c1d5916f225dcd6c1c3fe2b2880f4d42962befe3ab76bdc086e29381dd985206e3e00ce722c9c040af5ff4cd4a8183b446d91b310845"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,256,256) #11
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"f63292bab50668eb14b83975422a0c853fe55714a9edf9d8a817ba0b2f26ec40063a86ee3c79c694273342a02f68ecd0":"3c525956838e26b77b8cfc37f024ec398ed825076dbb749cf49a7d868c201e6d":"d9a41b47c3bf8743099dc8fd228f77dff01ae304761eaf57d751e11cf094bef1":"b790c37dbda20fbeafe9d1339a1151144253bdfbffe17ba87240eae49c606bf3":"3586b63315020b3ba1121314a0fa6c66d57de0ec44abeef7b7325e960832b7944cb0a81a747ee5c5d3163001536d3e5ad2ec869b0e5ceb14aee2e6915073619528c1421b59b80254dfc3cab0584898b0bca72c76ae25f52b7405b9dad38cb2b841e1d6a34fc5b277129db49928b2f6c0dd22900ee786ec128164ed12eb324b502499f1c5c89be2101901476b39c56034cc293e320e63a3e019186d4eaf9a098136e8c0ce7f6326f84ec95992dde2585ad3945a9534aa2954b8c15a48e3324d76"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,256,256) #12
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"3df74683f298ba48648714e384989145c1b84246736dc275636809d64c75ff603056e703c435eacf21c0bb152d9fc2a0":"371217ca2337db03c4d06714624fa11f90d5dc575bdbe12a457c610be066dc2b":"f26b9cac8df57a33e4b5868c36f2b9322994a98269dcbd7956b93d147dd0aa27":"0a6db86c3abdc39878045b8fc2d5f0f77a8e298efdacb4cb9f74762fc23b96fc":"ff5252b7a39460a73094b9d668b53d1932243caa885c0ecd850612fdbe7e46cb275d079bb75a6b050191282ccb11ef255d52cb763618c4b624560d79bb9a5bc99319783de43c152e7aa7c4cd879a75869285320a9b749c897bf07220cc1bef1edc494bffa6ab93dcf839dc15f6f2e508b9e216e2a1786b75abfb01bb7bdeda722b47af895f551670f9562d9f9b78e98ee7ea5c5ca4f836af5bf153925b2aec055eee8164edf3f7b72e24b1203cfae1834705f74cac8c6043a3c2abf6bdf28fc9"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-384,256+128,256,256) #13
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"53d70692f0f4dbda23d78660f0f08c7e70ca94441f1440348f7610
8874d13ea14652725abd1a94d315364416c90e662a":"6deee916ad660811cf05b5652f32df4e97f544ebb57762617359
159cc9a425c2":"acda427eea1c8c6791be6e4d2b60be30302abc84d5c5a13be7d510004b8710c9":"d27d7f598a14205c
45788665cd062135b6b65547d3188959e38ab675401d2b62":"f77f9de60e95da3f1d0d67b5dde29b31df59ce980ebdb
ad7b5e0a0051fee39e1d6fc4311f21efa016039bb05f3b009b223be6f2c007b468388a8a19bb468c7b82cc93dab3e160b
2b72fda1240fcceea01c2638e9c8bd2d1ed9ff9b55bf69fba4b6ae8e694c150896ac6233b75567993f9a9adf25ca0f0835
b9991ff4b8d3f4f1a3e4c5f9866d98b7a75196804f996492a61dbab5bf72f87658e2300a1b0777ef7f43ffe8962f6b6708d
2d91dcdf6b430cfaacb3289f74cb0f67370bcc9af249c"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-384,256+128,256,256)
#14
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA384:"85186650694f742c3f5f228f943788f05602d4827518908fd09a1f
b445d8333db2d65f376d48c66eb9e0498999e1ff49":"499928c41841324749143be9cc769899c38d6f6e6933e568988
96fabcd802931":"9574ca51f21865c2fb0efc75cc9d90ec5e9c43104979cd64d00ea5544ea01c96":"c0df840a18d7584b
62c70b2f057bf824168edb673cb517cd9dac89a0fc80c9b4":"b31e50202f883a8563cf129a0d5f8a33abad79d8ec8a971
67ed7fca778e5892480617cdf50b5e51547f7ec1bede35020a311572c61e33e9c82968e8f69586daea3dc19063bea5650
3f8ca482918d229949acd6f1c52cccdc5f7f4cd43602a72a5375f3aabfd2834ee0494823beada2daeccbed8d46984d1756
fe2207ca92186b506115f6de7d840c0b3b658e4d422dbf07210f620c71545f74cdf39ff82de2b0b6b53fbfa0cf58014038
184d34fc9617b71ccd22031b27a8fc5c7b338eeaf0fc"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-512,256+128,0,0) #0
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"35049f389a33c0ecb1293238fd951f8ffd517dfde06041d32945b3
e26914ba15f7328760be6168e6aa9fb54784989a11":"":"":"":"e76491b0260aacfded01ad39fbf1a66a88284caa512336
8a2ad9330ee48335e3c9c9ba90e6cbc9429962d60c1a6661edcfaa31d972b8264b9d4562cf18494128a092c17a8da6f31
13e8a7edfcd4427082bd390675e9662408144971717303d8dc352c9e8b95e7f35fa2ac9f549b292bc7c4bc7f01ee0a577
859ef6e82d79ef23892d167c140d22aac32b64ccdfeee2730528a38763b24227f91ac3ffe47fb11538e435307e7748180
2b0f613f370ffb0dbeab774fe1efbb1a80d01154a9459e73ad361108bbc86b0914f095136cbe634555ce0bb263618dc5c
367291ce0825518987154fe9ecb052b3f0a256fcc30cc14572531c9628973639beda456f2bddf6"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,0,0) #1
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"4cc8214cd7e85a76bfa735bbbfce926c0323fc348de6c05ed1800c
2c8f58c6b1001eb1f6b29b35242a3f8fa2e90003f4":"":"":"":"1efa15d644e1bdf34eade3ff2f5e9ca45203ccaa1e534ac9
b4287a846b71292b03102286d99f2be64b898fe909238f540ebc25f49522f60ef723a4c428ead530a97c62405cd5d9ecc
54ac5baa47ac4f6195d637833f462d21a659b4903d9cfa6c9fd4512445f9abb5782899a6bb64592f3c2b3c745b1864530
1fdb09a6a331e9fb6d9654fc79c14ed83ac1684c755b9cb209885f86ff290a71f08a848b960152f05b1aa8566bd382ddd
45521062831d7a0fb3a8bd8e112a91b5960690cd8585c1aa104514e3b9cbf52f6384e84c27bda2802fe9fb952cbf2bd60
7f869d0aeaa6b136c6a5f6e9b0522b6019b7ba6af6cff99fda612e024867decd8c0c6fde2034"

HMAC_DRBG

NIST CAVS 14.3 No Reseed (SHA-512,256+128,0,0) #2
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"d046270e6b7997cd5f4e9ed1193e55382191f78547a660854cf60
bb03d039a3950cd147a3445f6d32d14cbfb9da0c327":"":"":"":"cdfa9441aa5eb11fe3ba50528ed731c9ff9e70b78da07
5d00c52d0e281e3a868f66a53a2a6a272d7e0b1a32b6339f8afd108bb9e66b04c3d6bc069b7e01b69844322df7deac66e
605a9e2f43665b7932c67c418a77a4c9a302782d0e735795755613a1c5e90089f759d780fb3a984dee4e06ba3dc5a8c6
52549587d975e586a98ac6aba6563e2767f1a379261b9dd37992ea9681881ea7933b5c64093234c849142ced85bbe59
56f527d46ef091e4d18df2a6102621a91bca51bf7aa4b242414dc16e74ae59dfe560c19dbe315e7f98b11086bc26e336d
cefcb91c4828682da90d3921336a45fcd36ea4d1213a13213a132bf20aa1a3991b60b65de7ab9cc656"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,0,0) #3
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"8c7c80b169160c78104c205e4492a9477e6f7ba1c3bb4daa86d22
2deb6241bfd2d2dcd5c40b46fa553ca6a2f6be96991":"":"":"":"1658a7552e4cc98c228072801f9ba230123e7f1f7dca7
ba839f440e5f7570fd29c38b86a2aaca04cc87a56205b41d19e38998b47d0ffbfbd9bb56a6eb31bbfdce8d01e8991b823
15c39f60c222298160e8d9f14b1a6038d8eaf15eb7310b180a8e2e8d05ef028782b55d4782d4774160a39896d1a89682
3f8b92a99abb546ef02cf189200a1a7a2fbb7019e4d8a935224c20d11a18e0d8890549666f6599c261532b036051cf7a6
5dd33bc0aeab8fa2ac9ed520f6dd893b9dc3cd3b87d02a0543eca0bb52c58b7ac4ab3f00171e21dfd3363229ed362f960
d8a5fd06af5caa86018f9dce81ade6234a6992bfb9e2660d08a103dadd7d9ade4c45d691aa3799c1"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-512,256+128,0,0) #4
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"cd394508d86c384c0c998b58cf7017b7124269428e4cf39519b58
15cc2d88734fd2cbc87c79063db588d90b9cb1569f3":"":"":"":"7c4de5fa97362e63e52e790fb66d4b067e8cc1742975
ba6f9186295832d31c4e0c97b7dffa262b93b109621044a4bc89c9fc82211f5cb763974eb3a816fa7d7853577bee1c36c
2c36aabe28559d5bd85691c3e3bd610e61e4c3b76e167526d1331459d8bf09ceb403062cc97e1229eb3a70af6049d291
aadb002786e7d21b81c87fa68a51a1b9a89394788bab70783a88c883ca17eceaba455f357c611fb279e38f67e3c27c5ad
e5f95721fa79fc2da1bd44ca7f304161359da4e45d7b847672bc185ba502123a802535dbd167b2c93bf901626e23fcaba
03c4f89625a930caaaa30400645680e5931e094aac6f6467b90b13c2be9c98744f89d113151cd2ffb"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,0,0) #5
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"a14be417001030f6a9c543f829715b075d0efd8fa35acc7eed02a1
401c6f59dfc87b8b9255e62fcda6a35e52fa4a6f9d":"":"":"":"ed29a49be56e081f5b6abcd2ca1a16dc096071989de72a3
9b8bd544d2a2a2db5c886c0c29ce454cf60addb56cb4f28f959ccb7163280ef81e48dd2a02024c34a120301d359f03844
d1af01f485afbe7c9b17288cf345172290fdc44e124670c5ca9e8590df6f9f63d60849c62d3921003532dbe3e3e6bdd75
d28211365f6c489598a99e605ca671ff91552b5916ea9e12259723c0e1a633be34932d0c816c30b519c79656a70368b2
8fadaf5eb32eb6e47e00b04f152ace2eafc9a3ebd3b1b3795ad85e0897e46ab57c361fef2908041d365f73180b505ae242
6603decd0b7dd33e2f7ac885aced4194999602d4d62a984233d0696fff86f7fa7a6cf993fb7e5"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,0,0) #6
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"b8ceee088f3b13dbd1e7cf230449f246a456f504d63fd4288838a5
0ab76576a3f400502913cf57cb2341c5e6a63fe9fa":"":"":"":"b4fe3f6caedf4ac7b93fb1c2f316bafa58487f28a37b8400
fd1f32c963b04cb3c7eb601d0dd8a7e4538b14030fb0e97794c617366ca827e3afdb0f714983a6a72b261db8bf98d5fc4

8fb55158661f987d08e952913212717cf204a3e8cf1177f63e2a46d920ffcec4b580a1361253a689bf765200f4e90dc6b3
4a56e10cfdbf932fbc3b75da1d55cba0c5287f552d883763b83acdfc7fc9d762f79774701f7ace701f0b26c67217e022bf
6b6e0602e0d68cb1377b5ebccb9a8e41188dd1dea662663e8aa093787d6490a4e887a34a27309c64c40e4ab2f0acfec4a
1b8d419d99fb578aaa82da9166a7d7873e27226db20d313e868bcfa4fe3854d6fb34def7d6"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,0,0) #7
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"3c1e8a0199786fc268ee0ca0c0446d7363bd781069cf3a3faef259
2cba06ce1e70c7c691af73d6d59addbd6e3f646d64":"":"":"":"06f44bebc2c1736b5cee283e530bb877b28651d70983c
272a10efa80e3794ee428644048d67245dd3ca8b769b6bb192c9468a9fcf2b71c417283713d39e800225ba659c327302
2f5177fd7867173f457f3bb66ff2c2e7bb2574dfee54438e35c98506c178d35259b04e7c541016f5c2d980074b4ea8652
03ae2e8935d745a02ab5cce04d233cbc18719b1900f2e7e98229b851d19fac02fa6e5ac1bc973b20a17509739bd989d4
ef5a66fd9e19e3ceef2415b498843e93631b2b168167bdbb8db313eef4c9668d5001cb34767ee41db872163987c3bdc1
44637b52dcb767ffc19bf44fbad487b1eeae7957b497fd59a95f0988315eba73ab7206542f31c49267"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-512,256+128,0,0) #8
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"e8a0925bfce66dee7e6a54fe0311d259bd7f7a22b8576d64840cc5
1c731212cb1763365deab3ab82de9996e5c8570eb9":"":"":"":"63ddfd70508cfa247408ec231d56df7905f65b62e5e5a
8309fff5239620faa0f055d7b8fdbc648ded78fd567c3141e1723d197296c92d43fdc18af0c4a54fcd52613286c78ba7bd
fd0fcacc7b11b374739088323ba95f30872d77b6aad21228253133d76d29d0d742ba349956fe71e8bbf3fc7186a3f85f1
44a9040ceb0529a713583c1fcdee756d0130b38df0964bfc3b669fabb6ec6874d17d9ecda9fa567890e42540185eeb349
7ba8db80b803f63803442aec14735e9eda177484ad61bf0c76c2862b7691b4cc74efbe35203f8cf4f24aaaa1d831030f28
eef8b49e85b249e6fe835964d53aa74de6a31424ec3c833f4b8b39559934bf5f23d4b1d450bc3"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,0,0) #9
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"c493ad96bb20b2480bd3122b4b1ea51379f5fa2bfd8bc0fed40809
95b162c609b6d6197f432c8597163feb9c5439525d":"":"":"":"764d3e4459504b490eb1db7b5ab8e6413601e4497505
34f4c4f70025026f87217010eb14705eae6e513796c7f20ecace32a063238824b3fd6956810066930bf425a1c585221c8
f61ac64aeccfe8a3e33d164d02d5434e9e594b7ff451601874d268a2fd8de9922c36e67d8146fe553889a15f624d499a2
2f5109896758f30bb98f70eac11da1ad48e99bb4422acc5b97295094324eecf530525c1ba150886d053c84004c265693
a4419602e5e59bf120de6ff054d0c7c96bc14e9b5fe1290c08ebebcda21744c04a2e78964cb2b52f8e6a70930fd1ded1f0
edbda4deff91a3310019e967df3fdbfa228bec9897412a748201649328b7d784851fcb5ac1251f8b"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,0,0) #10
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"1e868c5fe4b59e6d4249854226bf1120a74386ea590e9c35c58d7
ccdfad56d71dbf557da684289e96cbdd66cbd9cb879":"":"":"":"2032963be29c0d24c2631b1cd895124b9801a4d5c14c
28fb34cbfb1c2467134f499153e2a3ec817cc4b2e4e06068ae78f5696dcee99334b0b51e9f29e56a3d3fd5c65c4cc70e10
f9e0cea2572c28ec4afe0896d7689322d3afd931ff836be485f78aa179100d43d910564dd1adfedcd32e3e7e53b06c0a46
a90b1173e4a5152cd8aa38f2a7e329d01c0b81e62be6c9fc8d1ff3db08f8c31c1e77c5d7fae619555c0e02c658486e35f2
7a7d58ce63b9b152b9ff528ab6a6cd9b59240f5a7b6b52dc3f6e47f9daa2cb8cb525d6760cf409ebe2c7641c3c32e3305
45bcd73da9eda20b7590d84831d4bec807a56994259bcd2fe28105f2d7fcdb3eec523fdef7044"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,0,0) #11
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"55bc1c7358dc334b26412ab472dcf4210740cfa0ea688812d8b1a7fb257b979edbab14240cf59fcc8a7007553ac480eb":"":"":"":"6a9d30d4ca97dbfc2d2852bef044bbfb95ac253b27e588c67fe179f6adb81147cc1cb6eba6a2c4afd6f8b3f1c8d45b51af1435ebf1ba8596830314353c9b4d8aff9620dba0099fe0a1ea417b97fa4c28491fe6d2a619172127f18155840f90456bfbf1e7ff587fbe566d6b8eadd6ce594bfcbabedda37858a7610c8230f594861984dbf1e3ddc9eccc8b9d2ec3cba1306d178f7677ed399b10b995b3ea55586519e5730e52ee8880ef0e63c476f2a80d77c6ba802c47e9174297b27520fb027d134e17cfa6f99d59cc5f53737cdc2e663e1ac59bf74a87ab1064e9acd4811c0406ec5a29a081bd0efd1e557d6b6c9c7fe6131c5c00fae82339a1fb90d3be2b6b"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-512,256+128,0,0) #12
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"d894820d9cb243859447cd3a3f6cdd125a9c4faece6ad756d288a15c5d24c39d776c5ea9838c4c34f39f12c1a9df6700":"":"":"":"ba23f7aa0b7f6a93bc0df32e68e78786fffb5acd7fbc2864468568753e3ddf31fc2187b20c229d0d0b261510f6442816d2226024b57306b474079c92c66a00be482fc104cdbccef0450b3f2ce94f6bb6a5125e0774a28a2a083f802d3c45e9d4253295f80ca4bc439f539a7f82eec6fd450bd196ab468ec6902752dced44ab557fcd3f6a72c47c0f18cec6545ac669cf432e2db308d70a7394ec772a34f14f26d7bf7d0bd7e4437248618efa2c08adc7de9231ddcc976ef8bcbd11be54dd17ca9fa515fee6827bf5efb602fe8f1cf5d67078b17601803c5be05c24edccad2837d0be191f918d6dc62742241728a8690db5836c2045ec9f8bfa87b768f4febf2f"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,0,0) #13
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"17facdf2fca2e1134674ea8e8daa609b4477f415c6a13a5c157f3fb7727dda6d3c1dd89ad63e781588e4b3f8cb1f2f6e":"":"":"":"f472b4c20bf07c170b3c8eb682469e88680d1fa5561d72b864c5c438c95c4c8a3e61f89fc30d5fb4e843e5ed1230778b48c467fa46ebfb7b56220a610483827f3f7f8ac307f8aa57a68922a06c8fa5de732a0d05835cd48690a2b3f734e4b7e74799ad774579a9eb296112f3e2bb68551af0e9e0e5e0bbb219ccb6c78459dc68a3663987156a50e72aebb219a1e43b5603dbd8055bf1e76a4468caee86489ac9a1a9a66ee7b193484ff3bea84341b62dab124a43e38945cfc99f2c4c15590fe180bb3e6eac544483aef710278213a83da85a38b6d140f33654c9d4f6b8ab3eacef1c57fd2237dbe8adf23b3aef6ab30327ca119b9e1e95ecd068aafae0d07a08"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,0,0) #14
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"2c13e44674e89aa105fc11b05e8526769a53ab0b4688f3d0d9cf23af4c8469bb700ac6a616c1d1bb7bd8ff7e96a4d250":"":"":"":"f778161306fc5f1d9e649b2a26983f31266a84bc79dd1b0016c8de53706f9812c4cebdbde78a3592bc7752303154acd7f4d27c2d5751fc7b1fee62677a71fc90e259dfb4b6a9c372515fac6efe01958d199888c360504ffa4c7cf4517918c430f5640fedc738e0cc1fcec33945a34a62ca61a71a9067298d34ac4a93751ddcd9a0f142748a1f0a81a948c6c6a16179e70b6f13633fd03b838da20f81450b4fdc1752e98e71296f1941ca58e71b73ea93e99a98f58d0892fa16de6a16c602036ac857dd75f9ac2c9185932103db5430e80cde9131e814a0bf3f3e7a2200a7152424472fd27f791a854f29aecc448f8d3fca3f93290266df3193d9e13e08907ab2"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,0,256) #0
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"a3da06bc88e2f2ea5181292c194a10b3db38a11d02ac2f9c65951d0c71f63e36c74e5e3d7ba0193bcd6839e9ae93d70d":"":"dbb7270760d8d262557807ce746ff314fd06598143611ab69b

fc7e10ca5784b3":"8cdea882f894e5fdc5f0a0b16b7d9ac8cde35ed17bcaf2665564d4ee74059e29":"cb706b90e88380e5c1864458454027821b571dfeba0da83f712efb107b8752099514ef87b4488fbfa3508a00954bb03090766d2bbd399e71c86c7967a4e8ded57095a29d4cfa01f8d28c97e81a4cd4fc5be7fb32a0d6c230cb8760e656b74fa7e18e2063ebee5787958b272fc5de93f0d6837e55f0c360dc593c88fff30a428cae37ded52f825646e04133a19790c304e4b1f040e10439c5edf454e6f71b23eeb43cdbe7b0634b8e283a97806073f7f28a43de2d0d969b3eda380c185b785b9101dc905025c9cdb499e594de0f0d3eb41922c20994fe2c403dd5bf01e4b2c3ee6654d6ab9cca7d4d5ae59525a796119547eae6a3cbf8ad0e9b1de3c4d5a804e4"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-512,256+128,0,256) #1
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"462cb274b7def1ac0f9db135c8fa2e48599cfe2badf2ae9f6d06886b25dfb0cc250461f0dadd9e23cc6c08ddf4ae12b9":"":"b087ff5e230284aef4c90b5f9c48fec91b486f3d936d422475a2b12ff47a05b0":"150a4ca383c3863d9ae3212de9ab9da7442fcd5367af157714d74c149f69eb9d":"12d4740dd0c5356fa76cc441f9088e361d3e636dc7b1ee27a26e28218eff470e28f51b76540939d624cacf2e3facf0967e7396a42017f68789e53f4b1d216fbae675801b8869b06d173d42126bf88fbbfef60aea6c4ba15538b2d64f8f22f389ee35e01e4ea88fd7c9e4d10c145a5f6e4dd33a55f2cafbd5f56856ea945b3b596b4900cf78936732bda49a52bc5a648c6561f48b820699533d48ff04eccd81aaa5bd25fa277ef314026effe2e65a9c38d45832cbb89579535782bf6299327339591a3e66d82aef6fcfa0a21b6b50a398b737a83a6a9b34dd46f3d15162dfa488fcadd18dd06f856f6d6c4cac2677eca641bd4e044ef4cddf6c95f1725fd8c606"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,0,256) #2
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"727337765db704e7b9d23dd139e63b5ac97adea990b7d04881b6b2de045c974a0265210aa4e336ac32f4b0a428ff272a":"":"48b452cbaeb990b6ca4ba64ae8f2a91d792ab83ad499093d9c4566ed8c7cee9b":"e7e32096873180e03c9f7bb33c5af4edc3fb9a36113275839302d40f0890dbad":"21c7d4c258778dce67f1a134670b8595dbbb0e036ae78484d7953f280f1faa5fb3bd213a54132a089a9d6f1376ca8b7064402409187acbd5de7e4d7146c1f02f73087a6c62ca6a7e736900a9e4464af0351bcb71b2e1f1cc07440cd74f50a61757f0b3bbb91fde9c898e62a9cec3dcaca0c94d5d0a8edac0f82b3c99b65d736884ffdd23fff1d9d6e8199254e784514fe3c34db51a86eeb06ef7dffcfba9f195c52cc4b2db53e0a6b1bdbed68d85822c6c03571482fdb6535eee1b6e26ce7d33433d3a1271c5b93ce9a31c9d7c805e3635e79682fa5f8e7894d8d16ead32e3fe8c625174a12a7b8623c0000a75c506cd367bdbc4e3da3b462938875050ff2271"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,0,256) #3
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"8ce3f77c4ba4f40d4eb3e80d03f9b138bea725d44f7a47f4a1f7ee3afb45c2a0e8fa75683ba03964a8e3312ccc6e1b66":"":"83260430843b586cfa50ab51120ea5675d63402074d45b0bf80dfbbec74fdc63":"0640b6427bdd6ead525962b228392b3c28abe131719feb0c0f738288ee87acbb":"d0a402dac648f7a53b5ffbebb1f5e6a12998c999809007f357dc568d7c653bd3b4da793d6d7ef802338eb36c7e4745655001f700c4ca68cda07d726dd088ed9948b2d49d8b50a72530dc9daa3387cd69ce32ca49dfa6cfca98f8a8b641c929f84c5f4045579dbfd3fdcd997068bb0f905f9a4a00accf06a483282e2eb99b94d78be46e07dc87903208bac0fa75323920997d9c4f9c0fa4cca5e6b1d69fdbfae8dbb52d659028387472c1a54283d074954094ae11bd3aa97360073ee033d7008e63b89e0efa4788eefa96ab726af4c2422b7472fa1efb7d95bec93fccb7351768625de30d9f5377610026b6f7f9568a9659644c7e68483672ca9ac8d0994efd68"

HMAC_DRBG

NIST CAVS 14.3 No Reseed (SHA-512,256+128,0,256) #4
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"96b0d3b13a65ae1010bf40e6e2dc6e6585db8fdb8fbd2b272611e51c62e1111ae93babde207a42980c9ac9018ab01153":"":"b67c2ecbc4d4c46c3573883b61311a2655cdff0e01a12a20ea0cfa4e91034c2b":"9ca69103d5af577da056d4d5e95f53be87aae4689918bdf0d011789f2ccba9b5":"63f05a9815c2671298e9caa06b0746767fdcc00884eb1b30e53b16593508bb75dcaff9932230913f9b62cd0361af168993ce7b6b967114e2612c8f9c376104633ad4eae2e968e455b96d1d5ed6928eee9acb21bb8fdee7bf525f143dcc624a66ad42f1bdbafc19b165284f2c771edc57dc9092ffae6ef8acb9f8fdba496607c54b07f3ff4d1721f45db43f8ed5c695716b405b57034cf4f87ab487a01057ed449bd918093c532fe85015f0c5856cbd7a440c33c7968dd25330f78b66248873959967e307f9c9697803e8b0939fae51870ec533ef7d17e227dcb68ccf270299e65ed8483b9077831e010e9dda3a50ef7b008a0762c8ac5ef42b7e2ecba450d7d6"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,0,256) #5
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"49913e04b653d82abc54cbddcdf898c409819dbdda4af93bc97b434dd1e319706504b1c76f34ca6d9dfb181c7057ed8c":"":"68b8f6f749ad588ff2c7477fd7c55be648134d57be6846674f2659d75785c39f":"cd7b2d7b24070e501843f0caa20666fbf963760893f4e277d944991ec965fbe3":"67ba01fe694d8f9621d47be0dd9119b8654d028e4c095347629afd02e96fbe6e4535d1666ee0331a6da79e703571ea0983a0d02051bd95dd130c7733012424b79a0bdfbcf72c9cb0c6d6ee408e2f0de45cb084d8182d1b8b4d389b78d0e3fbb7f3c8891ef522f077851b2463bdf1399d178dae3299a43b00f48cd1068e17f42615bd506878eef5fcd5951c24641b58f7a563240abbab5779db1e44bc2c66dd48ea7e746660042bf92b727d622bafebc05de309c24824ddd1d9ae86034a8694ae5962f61ab6e76b435c9dc8b370d708adc4d6fbbfc44644da3f4d4f24d3c95d958de143531c84b188445b6840775726c87b1b058dd8c14e4648973d5a91a152ba"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,0,256) #6
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"4687135763568418f6f30af400d37d794f712b10a42087fd832d840b9e8b1f818dadd1aba09e78a1925ecd9ee0d106f2":"":"ac00dc729c5526698fb80f685ffe93e9c25bf93b22424c15c20043e1fcafbc7d":"948555d8a6e0473a769b7019e6909a8565e386a624a47a1f9c96ff5e6609a894":"4f09384ba8a34f819a0d4473c3387f74299753fd16e386be51a5ee70d1b164be6fa53a3face06379da2d961bfd6ba21eb437bc77b527960352790bbc978217549006e7409b86ee97d6a042957d27a02fa5f04de94791bcd7d02cc6798bc66d3b6cd887f2a984224b3c279382558ff64459703d93b40fcdbaa7abe1bcdf0b95f4c6ec6583a86a41f837c6cbdefee3de4767e330cb2f4a0d8915f192f02c1ebfc78345f80d5e0f21185c647376d588991486ca9a8fe5c68d0b71a5f81b08bb112c56f69c89412f0282eb1bed0d05c959608d1eb6b1eb4a76a76ae927cfd8d651a651fe83668f24bc0d19e5de86813b16bfe8c771dc9f16a7d6d0441b3278de136c"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,0,256) #7
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"4ccc3c6cd73101efb7833ce1195b28b3aa3e5628db02be166f2a7f6bf7e8efdad5ff3f1c375ef981336af28252756647":"":"8396edacbe629826be44543bece17ede600f7f877d1138af5e83c3ec44b8b0de":"98545ad6268e604fedeacaa10b727ced0b0e284a00c29081a41c0d2e3675bacf":"c37ef92675ad963cf41ee5c14d882698082e8dda5a0ce9d50b8409c9f0d30d3294c7c625ef29c33f395de140405a6f9cd9d737a29d892b67e90427af24e200bc9cc7b5d920aa8a93d8ddd0b6f69cc98e303ca3a512b3d883ec542403d58bab1b4232c31696e72a764f2dc7b278bba02efdbd5413a08563833ef7a283aa6e5ab221d1ce5c7dd14363ecbeee879d157b6aefc8bfd2acc004d19eda7cb4b382e54bb725705b3f52ca5be08df445d8f6eb46353ef26217bd3c1b508f049e810fabacc0a75d717b2bea9f63cd

8d2fdffc27322eafc98e7de18a911ff44cd0e5864e0897f0550e3c48674d11dbecc9d6d4c42f7592fba440608ad479ed296a6ea6b1b0"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,0,256) #8
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"85ef33038e0bee3e40ce8eefd3648e89c521ad537b0c8003617824b08a154b75c89f036845a6f24fb9a15513ed28eda2":"":"2c675110a2bbcee5c6096cfd8f363441e3473664cf09577a95996928519a9292":"f1db097abed76cdbb1fe6aaba94bb51c2af8f43c5cdd2eafdf6b40a234d3897d":"beda7162fb3e07d96a5796f091388995894f69a59f06a0c7c8eb704b5dfcb82f7171d34628b116e1ceb0b180e6052d01fcb13510edd4050e15d6a8bb27a5bbac46d8847972f2638967d53d5b7752452bbf0bebb953a4e40212ab587b8e74a9599021c93071ac55a08feab70ee040c3cf32246857167f13473d20a38c8d6d364da4d1f043e24a65b2dc58ae2a56215a34081fe91bd554edf86a7d582b227316662dac6a71693806545760060fc1a204df40f1b5df92c7b0561507ecd95609fa5317bc43b1e9a40880a230fb4deb79cf4a7a2b97beeb9cd4c8c841d4ef2668d870eaa11f2fbfa0fb899a424f1600bd46778136dedd147f124dde4d64693233462b"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-512,256+128,0,256) #9
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"77a48fcd8cbea1be145a65c9e20cbc4e660dd439c7ec7e2dabc6f0430c5ba716182f05e834e84e89565714fe8ccf0de6":"":"1b838d460961b8f1623667fb316772cf50aa462ceeb58c36e2a6482ce7aa9f9f":"ccd4048bae7f8166c35e932cf3a09feb2f97dbb31af61a3fe5e4edb881ba6930":"af5afbb8d60d77c36c20a8f4c20b68ccd7fddb703d1ae83b5981605c4483e4f092329bd75aaeeb6fb4e6552540bd772edba5e5a96dd227acef73241257fe8774f757c673dc3370423de5a85b9118b5aa98682db6a89f520174a25e8e4b71f83ef432a91ddd8f69c1431c40d282d7e789427f18d9c5673131d5d3797d1335ffda64319d642f5ea5c1641092893a4008f076b649170916a03e06f0854848607c6c44a9f27bd3b17b293a914a86139e9a1b11c8652eae3757162f9f7161a2ee6f412a40002781e8fc8b80242331528225e70b9b23c6b2c970db12eab61bc290fec9b4c6c13d6454d7336f439d9b4b1df59248ab84e3a79d7f37df07e88c20f9ed92"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,0,256) #10
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"71cea1ba7a7dc792ca33288ccfb67570d9b1eab34e35296209db20c6676f174df4e062d1f660522881aeb11a651581f3":"":"c9667d28614fa05f112ec31487cdb3d925f2cb312202f7d85695a8f7336573b9":"6363dc485ddb9bdd61db33fb1beae9bfe2d0e7788a86b50774f8658bac094214":"e62486e1dc854f90b803635c1718f075cecf7fd44d1d304d0127979b83bee5e4abdae9076fc5ef89f6435e4b72cee056372c603f16beed39a2adf6ddc2577b32b29396db81e9ce57fb67c2525c2a59dea259ace4a7b6560ee20ca8e3f476786c34466ff5f6b45ccc916477f6fe96e7e4be23867a9ff9fa07609d9d8a5db7f5e1a068ba9b9c82bf72e76d17f73518affd5c58368232bcafe65096962c561617f489c8d978cb28676d8932a3c3489eb0f2f48a193826ee785dc850e41b0ced359ecd2636d96e83fdf8996617e6a39e141c124ad1e2e5fdad27144e60b56ed70d91543f3046acc831a6d56926ab1635de7e04a149958c9365a53c144903d7ea392c"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,0,256) #11
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"3a23653a34334db7d3abbf747d9d47d6b18589ab3516b0600bc93517d206a1a9c74a51766beec0563db655273d5dbcf9":"":"89922f45e6637e7fcae0a98d7ccdcf36650bbf7fe3253b7716014047a0983e98":"5d7519b3f442e1246185e1e7a56fd37473f18824f3c9d21656f54f1fa8d2947f":"fa40b69397e13d5f1ceaf294fb1d3a15db8b345286e5359bbffe5cd743ebab412845a9f5e4ed8481cea178d7b647019a7729c264220991c

3ae276f82d6c33402f061aabd2e28cfed64565cc2d7f1774e26281d0808b2857d1c144d5aa36944a38358181b28b9110
470601204076c02ed44ef411cd6a75fecf55225eeb3ef4f1717d3f5cdaec83f5defe835d2a236eb1a8f00167a727329163
eed34b3b34bade7896e2d0de1db1b15c7c2b173ee8d4f0bf77f8e8a973be61e107daf240b9b7edbc599469b5f40e98c0d
2d40b048ce4462cdead7e8f85d175a1f39f8bac61ec00f4cb4c8081201ca6319984264adca745b1d0feb471b5d8fa35bd
ed03357fcd7e0"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,0,256) #12
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"24cd11e75f2b0ab60c5b7a35020d716cea2e4f5b7748327c0cf355
b11805189334889dc3198f13c36cf7beb42b2a1a6f":"":"cf9571fecac5d79d65617a885815703de3459cf739db097f8ff
2ee557d0b0745":"2282cbdba64ac2a4053c070efd1dd0638fc31dff97dfa15f76bc077bf173a821":"1b0466ae577c0b9e
943616437c24b9d32ceeaec15bc83841843585c6255534a4a71ac96698f628d907255894f6199f6d7bf405afb0e46359a
e0dec788ca52111950f8adf88d324f5b9a76d79e67c3581b0cf0318901332883794398e6aea0f7da1f55f30ca34b11127
e885e86d787f8f8b3a1342d71f3738c8445707e0dea687baf759b261eceb4d661ec9bb006e9f08aeb1cc0357cd8df5269
43d71a6d73c9ae80ca69fcc3004b91dfdb2b6b8d0424c1cad81677d510ac7a51c1ce6f02b9ab41466e37ae0c2adfc63b3
1fc2e4693e467d3384fe359e9f0fd0f4d08f4a9037f3fd5495d895b6ed4121cca037c6aa87a5ccc5b856ee6151a900459ff
0ea77550e"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,0,256) #13
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"4931d76a7ceb2238c1f0ed76be24d2fe1a925d1084a392fc8c43d9
3535da0e9351e52abb58a9bc34c46f254b8313d387":"":"92a8eb05034555680bc937d0d958e820b09785009e5e05739
f29d9af17a63976":"d37465a30f837fe05f04f6b7ad4bb1c83bbae83f9c78f027b4831f5e2ad2dd78":"a61894d3c30081
c7836dee8506cb97bf7bb4e56a8a94c72d9c8b6900b69ea68b30c41ad33dd21554361c171cb959c555bb668436293e3f
1c103bb72509e43f2baa19742ed8c2d3eb9d0790c845097a7f0b2715b3d127a7f043c4b265b4d6fb4b9af9edd12427e1
b5c8b680a135a315761aa4a9ed598a7620f335fd595c40c933696cf95b7eca55e8520e9154f69e3446ea4fc3b69f36fa1a
e7eb456b350c93a1ebde342bd4578142d8338268af1c240c94457888d045d73196347318f89e281865b826837ca79da
5a6dbc81569c42da475d97ab5501a1b13e99058c40840958331bb73c78e5ec90aa0464b9f603f11bc4baddc28b71c422
82176654458d2fcaf"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,0,256) #14
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"ffa596ed725daea92273519c279d0a26be7f77cee1fc4fca44dc99b
97ad8125a3172e5a36ebc671df1fcaaa54bd7218a":"":"6cfccdd8253cc5b284701ef8d16f8888f79100373a7df50f43a12
2591bbddafc":"5795ae5be47a7f793423820352505e3890bac3805c102020e48226deab70140a":"4a398c114f2e0ac33
0893d103b585cadcf9cd3b2ac7e46cde15b2f32cc4b9a7c7172b1a73f86d6d12d02973e561fa7f615e30195f7715022df
75157f41dc7f9a50029350e308e3345c9ab2029bdc0f1b72c195db098c26c1ab1864224504c72f48a64d722e41b00707
c7f2f6cdfe8634d06abe838c85b419c02bf419b88cde35324b1bfdaddff8b7e95f6af0e55b5ff3f5475feb354f2a7a490597
b36080322265b213541682572616f3d3276c713a978259d607c6d69eec26d524ba38163a329103e39e3b0a8ec989eca
74f287d6d39c7ceda4df8558faeb9d25149963430f33b108dc136a4f9bfa416b3ceaa6632cd5505fe14fb0d78cf15f2acfa
03b9c307"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,256,0) #0
depends_on:MBEDTLS_SHA512_C

hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"e97a4631d0a08d549cde8af9a1aae058e3e9585575a726c76a27bc62bed18a4b227221d5fe5a5db9810f9afe56a3ee78":"94084b11d55e0f9c2ef577741753af66ad7a25b28524b50ea970105c3545e97d":"24c81d4773938371b906cf4801957ac22f87432b9c8a84bc5ac04ad5b1cc3f57":"c8c878451e2b76577c36393ca253888c1038885bbfdacd8539615a611e2ac00b":"761422dea283262998c0ffffefc77de2d395c818b9cf1ac2bcd1153235e0d8b63199c51e195135a75f1f87b454484ecc560c532c7ba5923c9490a423c177453459d81efc38ce2939226043cb733062eae303a009b48ee0cf3c7e40abe2b57a70a6062c669a9fbff20b4c94b4ecbc5f744a80d7be8134359581d441da921737b1329470b214f3e679fb7ad48baf046bac59a36b5770806cdef28cc4a8fd0e049b924c3c9216e00ba63c2ff771d66b7520dd33a85382a84b622717e594e447c919926a5b2e94d490ee626da9df587fed674067917963fd51d383e55730c17a124555e2e46e1395c9920d07dae4d67ffee5c759b6a326eec6d7b3ba6dee012e4807"

HMAC_DRBG
 NIST CAVS 14.3 No Reseed (SHA-512,256+128,256,0) #1
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"5c96609e9de807efed31d3c2d63e284be5c44c1b5ab84672664de8d8d8e2f8181b95a5290fdafeb05dc902a9a7bd639b":"135aafb3bbc89ef1e00a2a35ef32f122b7511cc55d86e7822a34859b630b4d29":"115774904a953af07936e3efdcf6054b4c534dc8654f563bb10610444d30625f":"4705ec7525e63919f7483fe76cdf7397b19f22d2a9d54b6cf0ff9abcf0a7c46d":"ae2cfbb29fde23e8c22d77d7a50ba66798da93be4e49ef78b38c9be2411e2d8a9954eb29fbad0a967c51b26d8d746801539aceb32e2459d07baa994869d3b6db2c88fb9d7250fac00de8f79990d501ad985590031f7c45a00cd9b6d1b5531b238f3a31d33237c40a3da31356171cafd52cbb7929e32b38fe523d8212de801f554348a3cc468daca70e05affc9af97f172aba00b2acc50d7dcb5f0ecbce741c71a65c657e9d0f250c44f73865962b1a0d19738e9ffe9f17c3e03363bedf5312c444375529fa8df9dd72b7c09f20c2ef37abb93e6fa57cadbcd7b23036bb9924fcfb9bf83b09ea360fd3988639151b1ab22939e9ea1cdc413f7a2cf04cf2778345"

HMAC_DRBG
 NIST CAVS 14.3 No Reseed (SHA-512,256+128,256,0) #2
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"4cbbd0538535994cf00354ff8609ddfd04e80dc4174b9542cdab52385dd968ddbef8157a6e3f26f040229a450f8e564f":"ed81729d1aef522f7bf9c127207d8a680ce4432964ed4025b5bbb12964374f3e":"1259073b57358935b7149fa4349793c5ff28d3ce98b483ec48986aa285451abc":"b350a4e931bb5db50a866aa3c01ead7d48d5859bb97b675e77ebb844ac832eb9":"215cca589f737df48d60360c4806ed548d44938c2bf5b1707310df987edda51e5092a7d9ca4955303ac59bfa980ba6e1819ed1141978c3d7df1125f5c4abec5b15bb8f5fd0edb1f26bcebea5aa7c8d5d32e8a5b608f609d9dfd765074b23cc524596a91226b726d899e42bdee0321eeb2dbaf63d33cced6890c19b466636df05072f007ae60a2364dde7f82315e3e30e63258b8abd12f18b6ab3d384cc9349e56dff00c3f53a86a301aa7205394199d32382096f6cd9db9646a92e73c3fd1e53c28a91683031c1ac72bb85af50be669d0e1d7b05a3bf1fc9720025c1e39e1f09d18d2e9247f726ac691a1c2321a667e6bacd7d77a57ce46397db1a91e7908ad5"

HMAC_DRBG
 NIST CAVS 14.3 No Reseed (SHA-512,256+128,256,0) #3
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"9b2bb0f34e6f0a31eff00e6604e6ca77643f69895877f77197a06e2b42bf047b3c1ee55a2a28fb3579324a54458310b2":"895e7060956784e5ea113ca785214bcf608e2a53c175e6edf5b78f1ad90e67c6":"c0b1980d57fb797c4907aad1fb5662bcc8d6ee30f6bed951e77c11d1893346e9":"af3357fd21fc04d1d1bd162b94bf129c45d41fee90366a180d98d41325336b5c":"50941cc105c694dd26d5bc73c08399168a270428ef594a6968fde834e889cfbbf0a80d7dad65d2fca21ba8019f1011313fe86983a555fb3ccb643bb771724e04114f3266d72c2e1a75363aebda9871c3bafcee3f389ff4c6f1f1bb5e6da5389e04f2822da800cb058da9cd698c65d54b16e7562c83506b632e4b5c7a78d6e36ec307e48cfec4fbc3ca3dd67ca95f9bd7f1d609e0a6d8b5bd3feef00e0c4165e77da84f989210c78daf633aef657855fca26b832994000f980c21d355db10f71f9cbb8079c48aeb673c5ba097a325d9a89e05bbf960fed4f8eb097cf37f61900db8171685107d53f85bbd8c1a4a1c7045c8b6e3a8a2c4114542292555585a090d"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,256,0) #4
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"9c8306c6941098408c56518a44d3075c22e02f19a6041d2e9c4e2
96fda435db917c99d538ab65f6f1bfab0d479a1833a":"3a80e9f5b71b242ae07ce7b617057dabae189c5468da2cf049b5
b529abc877d5":"3c151e92dd3121a8d2d11604632df00cf90706d3e843737445de0f2fde1ea924":"f53cb5fe673201f5e
af4115382d48ba45be405b37a31a56e41d1d76202038b06":"9bf31156e54d7142490e620afec2217931fb2389215a360
9b384b0551bb3c9d90c3b3053054046a324db9b34633e41b66114bfa7ee86bbd22d08d53e349a4dc875265b32151d3e
475df348a22d5226478184f372b0ba3be92ec1b284fc66dfa3609463214b6b468b29478acb0c55e1d4674882cb75e3ea
a3a66ea0f4d7b1a571206a761d636bd3519afb6f05a0f1b6bb38c00bd68530a6c9b445b6b4a9c7457a055627b606f450
8ed676fb5ba0d27589b7f464271c3e561215905c50ec48f5ddd1b8549e8d163453083db96c7ec8eeedaf6804369e7676
0b08abcca937c497900be385db8804b443e8a1489b8f3e3e4cf367dac3e15cb8e95cdabad04f08856c"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-512,256+128,256,0) #5
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"87a8fce521df0a2e26f1b1f9c7ec9e98968474915a085a95cbdca7
d8c669e08a69b8c3c3df07f9ada368be448938bf92":"b1bfaead04743bdcfdb193d32260918ff803abbcc0d5ddc50439b
d01f6e42a3c":"12a07384e9c74fb3f33df1a089dddb7d416151a0270d0c0216e085f1ec4c249b":"9b42567093112cb58
89703b77b4b372276b5bbccadf86eeb9ef6d3cd395b2acd":"5ba662260aa0f743a33a9b552ce41d93335a855a55df11b
870efacb7f75e39c978e730acce3664c814ac10fa10989fb00a39b584bb14cad2c02c309703c8ea8768d479d9b4e17402
ee38cb82c5f4d80125f3e674ac1adb919cc8a988f79f531b08253fbad0a1b27fb1997a4e2c7bd5ff3abf66281e8b609875
87327a9101b76cd13771e23ee2f02dc339589b9aac4f5af740afdaf494021c3504fdda8f93f77cdd8262df7d4c48f85b6e
b03a7e5279db4d18f645a63eb6f53f9fb123c53a78686f0113a209b6eeef3b10cd4489875a07af863c467f25b69cd13b8e
72847465fba025e25fe7bcb41745369f255df0eeffc3e5f066815ef7715680b104e20a7e9e"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,256,0) #6
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"69d667bde79e41cb78742426ca5ebd48086cf1ded5cad7293fcf91
0e5ab23cc8cad75bd989c3ffd05817d1aaa5493c05":"5f72346eb50ea82cb111d5b3c91dc9b7c61c92fa1a062177d513f
b616b1226d5":"0465b8aa89d9cbbe8e1cfa2e64e64b8d1f5dbec7f710a6d37fce898e3f81e57b":"173135f31c2320cccf
513e88a21f2d207e00cbe4330d2f550e0be77405eef47a":"34a08d7a564515a918bce93cae084f27a558f6f214c4bc916
9dbf507c3f11d02ec97bdfd777960f6b4c4543c1e14456d0079215320ab607e04b7519090ebaf3a5fbb0d7a3fda1af6cd
8c5d785524bdba75abbe50e3d58e5f05f8f6b2c2570f1178acd2f4c11a7b1b8b4ebe4ddb71a85bf19bb2fb25241374530
cbc6c0605066e1129a2d398356cf2ec2f7a286c5b869c702aced63f4e12f39b7ce250547a922872c36268a3a4649f6641
987bb7c6baf1a3e82cdf04d11160ba11c5a002cfbcf4a8698286ff318ec01fc2c5f6664e50561991a533ad183a21e7b97e
0052b0350d213738b0c6e5421a524845a861f539930540cc40c6ed78c46be9c122e7974d35"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,256,0) #7
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"f1f6e5a55fb2180de436d48115aa1aa38a6242eeb0959de3690f25
9c1d8395a5862d1ac4843404d25215c83bca90f44e":"f467ef083c745a1bfc9be44f1d468b2518e3ff1c0cee6819fdde35
4d4071b17e":"fdda9f0888c4439cded15a768300d163c1e326ee5571c22ab95ab3e44b1676d2":"6b8d60c565604c8fa8
d7adaf0b07ed268a491fb79794d2770356e191daa1cb50":"55d0788614b770f4b8c3d3ac0bbf628f294ba2fd16612b65
d0f469ded665e3c8b82c95db80cc6b410b5a6e624151fc50bf02f279ffabc19dd094cffb17ba44b11209b923df326db14e
ee35a8bf1eca3807afae918206e844e517eb32c207342008a0da742e734433867fd86fd89d27ec6e51a9db3ad1adea645

fdc57179c4b71de8b455ae00efc09328a0bffd8c61e3880c007915997daeed4adba61b44040f6f9b6c6427e1c23357c8f7
e18b5c974b3c34a2fd5cb5e70f48df2d10c1deabd987f8390bb33858d9a5133a7bd798b1c7741729b8562fecb3d4831e
9ce101de192d64bb5d757cbb21090d669afc5566c1d6e25586678b5f2fc7d6c6113ac4eb54f"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,256,0) #8
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"0db9d437153149e101d5818b263b975735994dfc33d8b3f158a05
760867757ab438a5024e1d43006226018c378af55d3":"275bdc5fc78b0d8afb5c8aa5f7854c319a81bb8cc9300210a99
90fb7933a352e":"809da54d1830545672f180fa3e0441a0d3fe472e7cd7a6d707fee5af7e9b21c2":"ebe66cee6efbf583c
881a25e346ca7d99741dacfce0d8785c659e92774e26ff2":"878a3d109d814ff4a4935689ca96b3d444bfcee9edfcd903
1255ad2538871027273bad5225864e84f3c2afaa22a40e7f6793abbc49c8b0ddc7b30d9dc7b408888e6b98f4bc79e087
75b599661ea4b50669132c21272f8d17fec9d1e5310335b0e6480d7075c830a44ea528900f99de61191b5a006ca43403
56dbf20c62e8ffd0577d623146b12937e84a6e17c0ae08efd339c9aa979c7e21e9c56e019f7e4f375bb601b1a83c21f27a
554ec05191794befe514dfbff5a3c9a0a9c80bfe9b6adc7deffd31c70ba13fcf170abd6bf3d384381e0a31fa9c81b1bd207
ea2e0b4153b6a1252a9f73f19f6f099fda0f87baba99b9711a00b5f50ad88d3bc1c4e806467"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,256,0) #9
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"4106f6ba6a291fa54e4ecfd9fa61b961554e4e8e03e19d9bfd82bd
35c3471e8bc5bdcd2f810079c1bbfe906929e88d27":"5a7e61b86ca70939e64af613a667695c7c915e667c79998e76e5
5eb33fef6d86":"86c7d5883aee568aa74d25782019fbd6f5acf4196752ff3d1dd96ec1e7436424":"3a5d80e739f5a30e6
bb507d82b60ff987d5bd9cbbff4b47daff278a3252db3ef":"fb146146f828e880c6ec7ab5a65fc8ec4e4d7d975c6d7c0a9
bc7ce041f49799b11e235d7ac5a4ec4eea721c3323448e686ae96579233ad698a9d6fe3f5b37d87ccfce640192dcdb51c
7bf35404c90b705bd97482d95d1c3e3a40152c86ab923588842ab02f4d922318a7fb84453b072c749a7f54e8ad005c29
c48af6f01ecdd8fac13295e42b2077c70c7bf54e214317f98003e4cde07755e95c91f1953b29b3eecd49dc753e74aaf2b1
c83feae87428be6a5aaa3261f0f65491e04c1fcdfd5481eadab68f057df3c83694c7451fded86a18470b06f1779c38efcac
54b576e99eced3b5581eb5c9f7b3340ad5667d1f0d3fead8b9484a032d5f74d900fd64d10"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,256,0) #10
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"5d1fcdabb70dad1428c8be291720c92b8565f331ee3438d79bcdd
c968efedcdb9319f5ee91124b93b965d504211fef04":"6c8c8a066c6208dbc18a40a30b9f689048877e038bf76d65acbd
de7ae4c566f8":"bfa2e9ebe0d70d3b62cdbd78c775a62e0e22fa75f168123a336b66b9a2b68c06":"e48b5245ea241baeb
7f665a9daaad662d7b2422c3e3711cfbed81d73691864ee":"1586e0761c4a39013dcb552a0e363e709f4303c0e575653
c9b240be7449ea26e4bb1dc93f06ec958b6c06217757fc550b356c135063c00fce9d856aec0edd20735b46b7c9a8e7df7
80db3072fc2b314fa5cda653ba3690132f10d30ee94c8458846be75659ef3868086bcf54ff55a8db1ea65c3e747a8ddab
3f2304738e0c75adfc10c23ba651ccf0de64a39cab3beef667f466391a61a87a981afe883f09c4edbd3eae98d51cd3e7b3
1ee179f8a4e10feac96ea210a4b8415c9f2cfeb2bc8bf51f13801dc542ba1badda1c30141d72abb1bbb35c9bb481d91db
5691c44bf3526a02d0bf776304a951858aa2fcf3f45bc656abcaeea94cbdc851a914b4b3a3ea"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,256,0) #11
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"9fc58d0785adbf033ce6642dcc9a861df44a35e89d06b346b16507
4a048b500994b4c0b3e27306b8c805c97b0ea14bb5":"e02f7a856266195fb5f4810232cd5c71a4465e1d95625c01e8e7

eb69c63f6796":"7cd18b8d035b57bd01464280abe891b7faf55f9ed9910d9a148b030340c67cdb":"918c4d43fecf9932
27f7c120d239a30d3c315602800d6d58b9e9e0715964cfa3":"b8a3581eb4a208d1ab8f0e84e9ff3d2e0ba57703a7b5be
2e4f3a3ede2e2519f5e6068c28c41171446cfbc40b48a97bc7a9a1e4d3b02f48fbf55b1d63da7cbc5b7a95f354afda273d
bf5bf099961db4a4c5f296286dc0a51091a522398973d5527b2e55e0523c21fffdd0dd38527bc45959d5a711d541634e
3139577312d678421eb37553c127beec64422316e48542a906cd7efe0d96eae3c4f2db7666083d9365a76cee4a207d71
2ddb04bf775be29ed9f030eade4537961737e3939a19e0769a3a8b96d055120c49925fe1ebc4a2ad54468421dd5465e8
761b3e2e384373a971e408dd3a54907538a7d887986677eb192761959a4293523f81647a657aaeea"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,256,0) #12
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"d43927d1e633fc3433536cd03617a97a3a10a7ecad3f0c7816028
29f8ec7feb2dd5922f2a2dee51db93bcf35100a8364":"3335a02aba1ea28d2e56973e21109e0adfb5068613c447e625fd
83a8d0e34494":"bfde33c52407d3137123812c4818ca1e4b61878b8f9dbaec47935e3948a88d0d":"42597cf03bbee0e0
03d8677159918f5318402f7329f08e1d93c850e2a2a2f1bb":"e53c7d0b376a94809f472961acff314079014958935cd6
7acc476abdd919a43cd3f7d1462d0d6e628ef5d0c8e04a6d243838c61ea36b015e84d7ad59e49b45c9b04f6ec78687ba
47156e429b2fb6dc2c0da4f5677d1f689cd28612cfa6d95628c26b5b3e01186153a1c25c02f5ce5fc287623358687d203
4347b2433ffc1445a2d93cb0103ccdaf0c585f7f4e7d41aef310be127208b3da90523aceac5fa13ffe77eaa4d1fd058957c
8dd2f355cae7f9e3d8f29ec7099599ba6c755689d53d6ccd84e33407a066506d97decd7e306d22ca6e0faa7b94f91f4eb
004422ddf9dd6b1f49b6400ea55d40e25c67103ab50bcc92d100e89ba569b6d51aacddf02daf1"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,256,0) #13
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"0bd69ce9a0a66dffefba83ae563e8df0fc6c7d7bdf491bf52cbf3f37
77025cdf92b32217f550a1fe735b8519b44b040d":"820da3187bc879cd1f40476fd9677f3b67e02b35b6632ab68891e2
5f10555b69":"903b882de013695b4683316ffbd7c7809288d54c72e369f70cf172bff85e5629":"cfb5f494e76486ceef1
2dfe1bafd6ccf9b0754d8d2306fb0c41c0f4e921317ef":"ebad5e5a358ceab806ae5590d80bc0ba5d4061f49f4cb79a8a9
da4fd1e8cb8f41cd8edc657c5180d18e62da2b53a50085b7e18b957eaf4edc975ca9d43e380434f51542dcfa947c322c7
08f3d3593c520717230df17f9341f02a5596b2058a27ba23f72a862b391be884570b22e20c80dd20d0a935f068465d55
4c8291fcd88eff608e92200f90cccdc82cb5697f0406654d9582e8db54225aaa28697bf2c4f47eba086a575298b991098
c212c9e8d95bfa48f7e500c7223d9cbffd1df6f725909ab6e9aa837ff9e69158af434d18e5a7f99d1aaf10931f380d88344
ad841064130cae50edf8687615743735f80457a228475bab7559015c4f45f91bdfa31d87"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,256,0) #14
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"45784684d6004731689e33e45b344d7b68dc4fa841133cb2dd65c
4b326dffa901109dfac2e48bf17f2fea33b412dc653":"7c6f4675f7a0b8c424d5be9e809efa305493874d9a950cb343afd
fb64e77ecb5":"2b2dbe3834d8be93f1396b19be83bd96823dd82740da71c5eeb7b21865021884":"49c322fc1bec86d3
e20628d9bdc1644e6f5e0237c7c694746bfee32a00145696":"9110cec7d07e6e32724bf043e73021b3ca0e4516b619d0
36ac9a00914e12f01ece71989f55c1caccd542c60a9cccffb91e203fd39dca2d92c8eb03ee7ee88abf21dc6891de326c31
90f25ee9ab44ca72d178db0f846969465b25a07dcc83777e6b63a7f9f1a8246dd31ce50cd9eb70e6e383c9ad4dae19f7c
ec8bfe079b36d309c28b10161c28b8d66c357c7ee01f07403a596366725fd5bd3a5de3cb40dcf60aac10635615b866ae6
33fbdb7ece41695d533757d9d16c6d44fd170fae77c15b7426ed6ec8c9d6e9245cd5e19e8dc3c8c7e671007ce8454413
bd07407e8a2248bee95a7669db6ee47377b4490a6251abb60cd4e2e404ab88aa4948e71ecec50c"

HMAC_DRBG

NIST CAVS 14.3 No Reseed (SHA-512,256+128,256,256) #0
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"e97a4631d0a08d549cde8af9a1aae058e3e9585575a726c76a27bc62bed18a4b227221d5fe5a5db9810f9afe56a3ee78":"94084b11d55e0f9c2ef577741753af66ad7a25b28524b50ea970105c3545e97d":"24c81d4773938371b906cf4801957ac22f87432b9c8a84bc5ac04ad5b1cc3f57":"c8c878451e2b76577c36393ca253888c1038885bbfdacd8539615a611e2ac00b":"761422dea283262998c0ffffefc77de2d395c818b9cf1ac2bcd1153235e0d8b63199c51e195135a75f1f87b454484ecc560c532c7ba5923c9490a423c177453459d81efc38ce2939226043cb733062eae303a009b48ee0cf3c7e40abe2b57a70a6062c669a9fbff20b4c94b4ecbc5f744a80d7be8134359581d441da921737b1329470b214f3e679fb7ad48baf046bac59a36b5770806cdef28cc4a8fd0e049b924c3c9216e00ba63c2ff771d66b7520dd33a85382a84b622717e594e447c919926a5b2e94d490ee626da9df587fed674067917963fd51d383e55730c17a124555e2e46e1395c9920d07dae4d67ffee5c759b6a326eec6d7b3ba6dee012e4807"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,256,256) #1
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"5c96609e9de807efed31d3c2d63e284be5c44c1b5ab84672664de8d8d8e2f8181b95a5290fdafeb05dc902a9a7bd639b":"135aafb3bbc89ef1e00a2a35ef32f122b7511cc55d86e7822a34859b630b4d29":"115774904a953af07936e3efdcf6054b4c534dc8654f563bb10610444d30625f":"4705ec7525e63919f7483fe76cdf7397b19f22d2a9d54b6cf0ff9abcf0a7c46d":"ae2cfbb29fde23e8c22d77d7a50ba66798da93be4e49ef78b38c9be2411e2d8a9954eb29fbad0a967c51b26d8d746801539aceb32e2459d07baa994869d3b6db2c88fb9d7250fac00de8f79990d501ad985590031f7c45a00cd9b6d1b5531b238f3a31d33237c40a3da31356171cafd52cbb7929e32b38fe523d8212de801f554348a3cc468daca70e05affc9af97f172aba00b2acc50d7dcb5f0ecbce741c71a65c657e9d0f250c44f73865962b1a0d19738e9ffe9f17c3e03363bedf5312c444375529fa8df9dd72b7c09f20c2ef37abb93e6fa57cadbcd7b23036bb9924fcfb9bf83b09ea360fd3988639151b1ab22939e9ea1cdc413f7a2cf04cf2778345"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,256,256) #2
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"4cbbd0538535994cf00354ff8609ddfd04e80dc4174b9542cdab52385dd968ddbef8157a6e3f26f040229a450f8e564f":"ed81729d1aef522f7bf9c127207d8a680ce4432964ed4025b5bbb12964374f3e":"1259073b57358935b7149fa4349793c5ff28d3ce98b483ec48986aa285451abc":"b350a4e931bb5db50a866aa3c01ead7d48d5859bb97b675e77ebb844ac832eb9":"215cca589f737df48d60360c4806ed548d44938c2bf5b1707310df987edda51e5092a7d9ca4955303ac59bfa980ba6e1819ed1141978c3d7df1125f5c4abec5b15bb8f5fd0edb1f26bcebea5aa7c8d5d32e8a5b608f609d9dfd765074b23cc524596a91226b726d899e42bdee0321eeb2dbaf63d33cced6890c19b466636df05072f007ae60a2364dde7f82315e3e30e63258b8abd12f18b6ab3d384cc9349e56dff00c3f53a86a301aa7205394199d32382096f6cd9db9646a92e73c3fd1e53c28a91683031c1ac72bb85af50be669d0e1d7b05a3bf1fc9720025c1e39e1f09d18d2e9247f726ac691a1c2321a667e6bacd7d77a57ce46397db1a91e7908ad5"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,256,256) #3
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"9b2bb0f34e6f0a31eff00e6604e6ca77643f69895877f77197a06e2b42bf047b3c1ee55a2a28fb3579324a54458310b2":"895e7060956784e5ea113ca785214bcf608e2a53c175e6edf5b78f1ad90e67c6":"c0b1980d57fb797c4907aad1fb5662bcc8d6ee30f6bed951e77c11d1893346e9":"af3357fd21fc04d1d1bd162b94bf129c45d41fee90366a180d98d41325336b5c":"50941cc105c694dd26d5bc73c08399168a270428ef594a6968fde834e889cfbbf0a80d7dad65d2fca21ba8019f1011313fe86983a555fb3ccb643bb771724e04114f3266d72c2e1a75363aebda9871c3bafcee3f389ff4c6f1f1bb5e6da5389e04f2822da800cb058da9cd698c65d54b16e7562c83506b632e4b5c7a78d6e36ec307e48cfec4fbc3ca3dd67ca95f9bd7f1d609e0a6d8b5bd3feef00e0c4165e77da84f989210c78daf633ae

f657855fca26b832994000f980c21d355db10f71f9cbb8079c48aeb673c5ba097a325d9a89e05bbf960fed4f8eb097cf37f61900db8171685107d53f85bbd8c1a4a1c7045c8b6e3a8a2c4114542292555585a090d"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,256,256) #4
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"9c8306c6941098408c56518a44d3075c22e02f19a6041d2e9c4e296fda435db917c99d538ab65f6f1bfab0d479a1833a":"3a80e9f5b71b242ae07ce7b617057dabae189c5468da2cf049b5b529abc877d5":"3c151e92dd3121a8d2d11604632df00cf90706d3e843737445de0f2fde1ea924":"f53cb5fe673201f5eaf4115382d48ba45be405b37a31a56e41d1d76202038b06":"9bf31156e54d7142490e620afec2217931fb2389215a3609b384b0551bb3c9d90c3b3053054046a324db9b34633e41b66114bfa7ee86bbd22d08d53e349a4dc875265b32151d3e475df348a22d5226478184f372b0ba3be92ec1b284fc66dfa3609463214b6b468b29478acb0c55e1d4674882cb75e3eaa3a66ea0f4d7b1a571206a761d636bd3519afb6f05a0f1b6bb38c00bd68530a6c9b445b6b4a9c7457a055627b606f4508ed676fb5ba0d27589b7f464271c3e561215905c50ec48f5ddd1b8549e8d163453083db96c7ec8eeedaf6804369e76760b08abcca937c497900be385db8804b443e8a1489b8f3e3e4cf367dac3e15cb8e95cdabad04f08856c"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,256,256) #5
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"87a8fce521df0a2e26f1b1f9c7ec9e98968474915a085a95cbdca7d8c669e08a69b8c3c3df07f9ada368be448938bf92":"b1bfaead04743bdcfdb193d32260918ff803abbcc0d5ddc50439bd01f6e42a3c":"12a07384e9c74fb3f33df1a089dddb7d416151a0270d0c0216e085f1ec4c249b":"9b42567093112cb5889703b77b4b372276b5bbccadf86eeb9ef6d3cd395b2acd":"5ba662260aa0f743a33a9b552ce41d93335a855a55df11b870efacb7f75e39c978e730acce3664c814ac10fa10989fb00a39b584bb14cad2c02c309703c8ea8768d479d9b4e17402ee38cb82c5f4d80125f3e674ac1adb919cc8a988f79f531b08253fbad0a1b27fb1997a4e2c7bd5ff3abf66281e8b60987587327a9101b76cd13771e23ee2f02dc339589b9aac4f5af740afdaf494021c3504fdda8f93f77cdd8262df7d4c48f85b6eb03a7e5279db4d18f645a63eb6f53f9fb123c53a78686f0113a209b6eeef3b10cd4489875a07af863c467f25b69cd13b8e72847465fba025e25fe7bcb41745369f255df0eeffc3e5f066815ef7715680b104e20a7e9e"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,256,256) #6
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"69d667bde79e41cb78742426ca5ebd48086cf1ded5cad7293fcf910e5ab23cc8cad75bd989c3ffd05817d1aaa5493c05":"5f72346eb50ea82cb111d5b3c91dc9b7c61c92fa1a062177d513fb616b1226d5":"0465b8aa89d9cbbe8e1cfa2e64e64b8d1f5dbec7f710a6d37fce898e3f81e57b":"173135f31c2320cccf513e88a21f2d207e00cbe4330d2f550e0be77405eef47a":"34a08d7a564515a918bce93cae084f27a558f6f214c4bc9169dbf507c3f11d02ec97bdfd777960f6b4c4543c1e14456d0079215320ab607e04b7519090ebaf3a5fbb0d7a3fda1af6cd8c5d785524bdba75abbe50e3d58e5f05f8f6b2c2570f1178acd2f4c11a7b1b8b4ebe4ddb71a85bf19bb2fb25241374530cbc6c0605066e1129a2d398356cf2ec2f7a286c5b869c702aced63f4e12f39b7ce250547a922872c36268a3a4649f6641987bb7c6baf1a3e82cdf04d11160ba11c5a002cfbcf4a8698286ff318ec01fc2c5f6664e50561991a533ad183a21e7b97e0052b0350d213738b0c6e5421a524845a861f539930540cc40c6ed78c46be9c122e7974d35"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,256,256) #7
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"f1f6e5a55fb2180de436d48115aa1aa38a6242eeb0959de3690f259c1d8395a5862d1ac4843404d25215c83bca90f44e":"f467ef083c745a1bfc9be44f1d468b2518e3ff1c0cee6819fdde354d4071b17e":"fdda9f0888c4439cded15a768300d163c1e326ee5571c22ab95ab3e44b1676d2":"6b8d60c565604c8fa8

d7adaf0b07ed268a491fb79794d2770356e191daa1cb50":"55d0788614b770f4b8c3d3ac0bbf628f294ba2fd16612b65
d0f469ded665e3c8b82c95db80cc6b410b5a6e624151fc50bf02f279ffabc19dd094cffb17ba44b11209b923df326db14e
ee35a8bf1eca3807afae918206e844e517eb32c207342008a0da742e734433867fd86fd89d27ec6e51a9db3ad1adea645
fdc57179c4b71de8b455ae00efc09328a0bffd8c61e3880c007915997daeed4adba61b44040f6f9b6c6427e1c23357c8f7
e18b5c974b3c34a2fd5cb5e70f48df2d10c1deabd987f8390bb33858d9a5133a7bd798b1c7741729b8562fecb3d4831e
9ce101de192d64bb5d757cbb21090d669afc5566c1d6e25586678b5f2fc7d6c6113ac4eb54f"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-512,256+128,256,256)
#8
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"0db9d437153149e101d5818b263b975735994dfc33d8b3f158a05
760867757ab438a5024e1d43006226018c378af55d3":"275bdc5fc78b0d8afb5c8aa5f7854c319a81bb8cc9300210a99
90fb7933a352e":"809da54d1830545672f180fa3e0441a0d3fe472e7cd7a6d707fee5af7e9b21c2":"ebe66cee6efbf583c
881a25e346ca7d99741dacfce0d8785c659e92774e26ff2":"878a3d109d814ff4a4935689ca96b3d444bfcee9edfcd903
1255ad2538871027273bad5225864e84f3c2afaa22a40e7f6793abbc49c8b0ddc7b30d9dc7b408888e6b98f4bc79e087
75b599661ea4b50669132c21272f8d17fec9d1e5310335b0e6480d7075c830a44ea528900f99de61191b5a006ca43403
56dbf20c62e8ffd0577d623146b12937e84a6e17c0ae08efd339c9aa979c7e21e9c56e019f7e4f375bb601b1a83c21f27a
554ec05191794befe514dfbff5a3c9a0a9c80bfe9b6adc7deffd31c70ba13fcf170abd6bf3d384381e0a31fa9c81b1bd207
ea2e0b4153b6a1252a9f73f19f6f099fda0f87baba99b9711a00b5f50ad88d3bc1c4e806467"

HMAC_DRBG NIST CAVS 14.3 No Reseed (SHA-512,256+128,256,256) #9
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"4106f6ba6a291fa54e4ecfd9fa61b961554e4e8e03e19d9bfd82bd
35c3471e8bc5bdcd2f810079c1bbfe906929e88d27":"5a7e61b86ca70939e64af613a667695c7c915e667c79998e76e5
5eb33fef6d86":"86c7d5883aee568aa74d25782019fbd6f5acf4196752ff3d1dd96ec1e7436424":"3a5d80e739f5a30e6
bb507d82b60ff987d5bd9cbbff4b47daff278a3252db3ef":"fb146146f828e880c6ec7ab5a65fc8ec4e4d7d975c6d7c0a9
bc7ce041f49799b11e235d7ac5a4ec4eea721c3323448e686ae96579233ad698a9d6fe3f5b37d87ccfce640192dcdb51c
7bf35404c90b705bd97482d95d1c3e3a40152c86ab923588842ab02f4d922318a7fb84453b072c749a7f54e8ad005c29
c48af6f01ecdd8fac13295e42b2077c70c7bf54e214317f98003e4cde07755e95c91f1953b29b3eecd49dc753e74aaf2b1
c83feae87428be6a5aaa3261f0f65491e04c1fcdfd5481eadab68f057df3c83694c7451fded86a18470b06f1779c38efcac
54b576e99eced3b5581eb5c9f7b3340ad5667d1f0d3fead8b9484a032d5f74d900fd64d10"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,256,256) #10
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"5d1fcdabb70dad1428c8be291720c92b8565f331ee3438d79bcdd
c968efedcdb9319f5ee91124b93b965d504211fef04":"6c8c8a066c6208dbc18a40a30b9f689048877e038bf76d65acbd
de7ae4c566f8":"bfa2e9ebe0d70d3b62cdbd78c775a62e0e22fa75f168123a336b66b9a2b68c06":"e48b5245ea241baeb
7f665a9daaad662d7b2422c3e3711cfbed81d73691864ee":"1586e0761c4a39013dcb552a0e363e709f4303c0e575653
c9b240be7449ea26e4bb1dc93f06ec958b6c06217757fc550b356c135063c00fce9d856aec0edd20735b46b7c9a8e7df7
80db3072fc2b314fa5cda653ba3690132f10d30ee94c8458846be75659ef3868086bcf54ff55a8db1ea65c3e747a8ddab
3f2304738e0c75adfc10c23ba651ccf0de64a39cab3beef667f466391a61a87a981afe883f09c4edbd3eae98d51cd3e7b3
1ee179f8a4e10feac96ea210a4b8415c9f2cfeb2bc8bf51f13801dc542ba1badda1c30141d72abb1bbb35c9bb481d91db
5691c44bf3526a02d0bf776304a951858aa2fcf3f45bc656abcaeea94cbdc851a914b4b3a3ea"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,256,256) #11
depends_on:MBEDTLS_SHA512_C

hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"9fc58d0785adbf033ce6642dcc9a861df44a35e89d06b346b165074a048b500994b4c0b3e27306b8c805c97b0ea14bb5":"e02f7a856266195fb5f4810232cd5c71a4465e1d95625c01e8e7eb69c63f6796":"7cd18b8d035b57bd01464280abe891b7faf55f9ed9910d9a148b030340c67cdb":"918c4d43fecf993227f7c120d239a30d3c315602800d6d58b9e9e0715964cfa3":"b8a3581eb4a208d1ab8f0e84e9ff3d2e0ba57703a7b5be2e4f3a3ede2e2519f5e6068c28c41171446cfbc40b48a97bc7a9a1e4d3b02f48fbf55b1d63da7cbc5b7a95f354afda273dbf5bf099961db4a4c5f296286dc0a51091a522398973d5527b2e55e0523c21fffdd0dd38527bc45959d5a711d541634e3139577312d678421eb37553c127beec64422316e48542a906cd7efe0d96eae3c4f2db7666083d9365a76cee4a207d712ddb04bf775be29ed9f030eade4537961737e3939a19e0769a3a8b96d055120c49925fe1ebc4a2ad54468421dd5465e8761b3e2e384373a971e408dd3a54907538a7d887986677eb192761959a4293523f81647a657aaeea"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,256,256) #12
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"d43927d1e633fc3433536cd03617a97a3a10a7ecad3f0c781602829f8ec7feb2dd5922f2a2dee51db93bcf35100a8364":"3335a02aba1ea28d2e56973e21109e0adfb5068613c447e625fd83a8d0e34494":"bfde33c52407d3137123812c4818ca1e4b61878b8f9dbaec47935e3948a88d0d":"42597cf03bbee0e003d8677159918f5318402f7329f08e1d93c850e2a2a2f1bb":"e53c7d0b376a94809f472961acff314079014958935cd67acc476abdd919a43cd3f7d1462d0d6e628ef5d0c8e04a6d243838c61ea36b015e84d7ad59e49b45c9b04f6ec78687ba47156e429b2fb6dc2c0da4f5677d1f689cd28612cfa6d95628c26b5b3e01186153a1c25c02f5ce5fc287623358687d2034347b2433ffc1445a2d93cb0103ccdaf0c585f7f4e7d41aef310be127208b3da90523aceac5fa13ffe77eaa4d1fd058957c8dd2f355cae7f9e3d8f29ec7099599ba6c755689d53d6ccd84e33407a066506d97decd7e306d22ca6e0faa7b94f91f4eb004422ddf9dd6b1f49b6400ea55d40e25c67103ab50bcc92d100e89ba569b6d51aacddf02daf1"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,256,256) #13
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"0bd69ce9a0a66dffefba83ae563e8df0fc6c7d7bdf491bf52cbf3f3777025cdf92b32217f550a1fe735b8519b44b040d":"820da3187bc879cd1f40476fd9677f3b67e02b35b6632ab68891e25f10555b69":"903b882de013695b4683316ffbd7c7809288d54c72e369f70cf172bff85e5629":"cfb5f494e76486ceef12dfe1bafd6ccf9b0754d8d2306fb0c41c0f4e921317ef":"ebad5e5a358ceab806ae5590d80bc0ba5d4061f49f4cb79a8a9da4fd1e8cb8f41cd8edc657c5180d18e62da2b53a50085b7e18b957eaf4edc975ca9d43e380434f51542dcfa947c322c708f3d3593c520717230df17f9341f02a5596b2058a27ba23f72a862b391be884570b22e20c80dd20d0a935f068465d554c8291fcd88eff608e92200f90cccdc82cb5697f0406654d9582e8db54225aaa28697bf2c4f47eba086a575298b991098c212c9e8d95bfa48f7e500c7223d9cbffd1df6f725909ab6e9aa837ff9e69158af434d18e5a7f99d1aaf10931f380d88344ad841064130cae50edf8687615743735f80457a228475bab7559015c4f45f91bdfa31d87"

HMAC_DRBG
NIST CAVS 14.3 No Reseed (SHA-512,256+128,256,256) #14
depends_on:MBEDTLS_SHA512_C
hmac_drbg_no_reseed:MBEDTLS_MD_SHA512:"45784684d6004731689e33e45b344d7b68dc4fa841133cb2dd65c4b326dffa901109dfac2e48bf17f2fea33b412dc653":"7c6f4675f7a0b8c424d5be9e809efa305493874d9a950cb343afdfb64e77ecb5":"2b2dbe3834d8be93f1396b19be83bd96823dd82740da71c5eeb7b21865021884":"49c322fc1bec86d3e20628d9bdc1644e6f5e0237c7c694746bfee32a00145696":"9110cec7d07e6e32724bf043e73021b3ca0e4516b619d036ac9a00914e12f01ece71989f55c1caccd542c60a9cccffb91e203fd39dca2d92c8eb03ee7ee88abf21dc6891de326c3190f25ee9ab44ca72d178db0f846969465b25a07dcc83777e6b63a7f9f1a8246dd31ce50cd9eb70e6e383c9ad4dae19f7cec8bfe079b36d309c28b10161c28b8d66c357c7ee01f07403a596366725fd5bd3a5de3cb40dcf60aac10635615b866ae633fbdb7ece41695d533757d9d16c6d44fd170fae77c15b7426ed6ec8c9d6e9245cd5e19e8dc3c8c7e671007ce8454413bd07407e8a2248bee95a7669db6ee47377b4490a6251abb60cd4e2e404ab88aa4948e71ecec50c"

AES-GCM NIST Validation (AES-192,128,0,0,128) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"806766a4d2b6507cc4113bc0e46eebe120eacd948c24dc7f":"":"4f801c772395c4519ec830980c8ca5a4":"":128:"8fa16452b132bebc6aa521e92cb3b0ea":"FAIL":0

AES-GCM NIST Validation (AES-192,128,0,0,128) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"0c2abdcd2e4ae4137509761a38e6ca436b99c21b141f28f5":"":"335ca01a07081fea4e605eb5f23a778e":"":128:"d7f475dfcb92a75bc8521c12bb2e8b86":"FAIL":0

AES-GCM NIST Validation (AES-192,128,0,0,128) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"eef490a0c2ecb32472e1654184340cc7433c34da981c062d":"":"d9172c3344d37ff93d2dcb2170ea5d01":"":128:"017fef05260a496654896d4703db3888":"FAIL":0

AES-GCM NIST Validation (AES-192,128,0,0,120) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"fe0c3490f1f0dba23cf5c64e6e1740d06f85e0afec6772f3":"":"f47e915163fa3df7f6c15b9d69f53907":"":120:"14e1a057a2e7ffbd2208e9c25dbba1":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,0,0,120) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"4356b3b1f308df3573509945afe5268984f9d953f01096de":"":"a35b397b34a14a8e24d05a37be4d1822":"":120:"e045ecba220d22c80826b77a21b013":"":0

AES-GCM NIST Validation (AES-192,128,0,0,120) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"e2898937cc575c8bb7444413884deafe8eaf326be8849e42":"":"169a449ccb3eb29805b15304d603b132":"":120:"3a807251f3d6242849a69972b14f6d":"FAIL":0

AES-GCM NIST Validation (AES-192,128,0,0,112) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"75683c7df0442e10b5368fcd6bb481f0bff8d95aae90487e":"":"538641f7d1cc5c68715971cee607da73":"":112:"07d68fffe417adc3397706d73b95":"FAIL":0

AES-GCM NIST Validation (AES-192,128,0,0,112) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"0724ee1f317997ce77bb659446fcb5a557490f40597341c7":"":"0d8eb78032d83c676820b2ef5ccc2cc8":"":112:"7da181563b26c7aefeb29e71cc69":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,0,0,112) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"be2f0f4ae4ab851b258ec5602628df261b6a69e309ff9043":"":"646a91d83ae72b9b9e9fce64135cbf73":"":112:"169e717e2bae42e3eb61d0a1a29b":"FAIL":0

AES-GCM NIST Validation (AES-192,128,0,0,104) #0

depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"583c328daecd18c2ac5c83a0c263de194a4c73aa4700fe76":"":"55e10d5e9b438b02505d30f211b16fea":"":104:"95c0a4ea9e80f91a4acce500f7":"FAIL":0

AES-GCM NIST Validation (AES-192,128,0,0,104) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"b40857e7e6f26050f1e9a6cbe05e15a0ba07c2055634ad47":"":"e25ef162a4295d7d24de75a673172346":"":104:"89ea4d1f34edb716b322ea7f6f":"FAIL":0

AES-GCM NIST Validation (AES-192,128,0,0,104) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"627008956e31fea497fb120b438a2a043c23b1b38dc6bc10":"":"08ea464baac54469b0498419d83820e6":"":104:"ab064a8d380fe2cda38e61f9e1":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,0,0,96) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"8c386d67d7c2bfd46b8571d8685b35741e87a3ed4a46c9db":"":"766996fb67ace9e6a22d7f802455d4ef":"":96:"9a641be173dc3557ea015372":"":0

AES-GCM NIST Validation (AES-192,128,0,0,96) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"711bc5aa6b94fa3287fad0167ac1a9ef5e8e01c16a79e95a":"":"75cdb8b83017f3dc5ac8733016ab47c7":"":96:"81e3a5580234d8e0b2204bc3":"FAIL":0

AES-GCM NIST Validation (AES-192,128,0,0,96) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"c74620828402e0bdf3f7a5353668505dc1550a31debce59a":"":"cfbefe265583ab3a2285e8080141ba48":"":96:"355a43bcebbe7f72b6cd27ea":"FAIL":0

AES-GCM NIST Validation (AES-192,128,0,0,64) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"1eb53aa548b41bfdc85c657ebdebdae0c7e525a6432bc012":"":"37ffc64d4b2d9c82dd17d1ad3076d82b":"":64:"34b8e037084b3f2d":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,0,0,64) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"50d077575f6db91024a8e564db83324539e9b7add7bb98e4":"":"118d0283294d4084127cce4b0cd5b5fa":"":64:"507a361d8ac59882":"FAIL":0

AES-GCM NIST Validation (AES-192,128,0,0,64) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"d9ddca0807305025d61919ed7893d7d5c5a3c9f012f4842f":"":"b78d518b6c41a9e031a00b10fb178327":"":64:"f401d546c8b739ff":"":0

AES-GCM NIST Validation (AES-192,128,0,0,32) #0
depends_on:MBEDTLS_AES_C

gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"6ed8d8afde4dc3872cbc274d7c47b719205518496dd7951d":"":"14eb280288740d464e3b8f296c642daa":"":32:"39e64d7a":"":0

AES-GCM NIST Validation (AES-192,128,0,0,32) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"80aace5ab74f261bc09ac6f66898f69e7f348f805d52404d":"":"f54bf4aac8fb631c8b6ff5e96465fae6":"":32:"1ec1c1a1":"":0

AES-GCM
NIST Validation (AES-192,128,0,0,32) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"23b76efd0dbc8d501885ab7d43a7dacde91edd9cde1e1048":"":"75532d15e582e6c477b411e727d4171e":"":32:"76a0e017":"FAIL":0

AES-GCM NIST Validation (AES-192,128,0,1024,128) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"94c50453dd3ef7f7ea763ae13fa34debb9c1198abbf32326":"":"1afe962bc46e36099165552ddb329ac6":"b2920dd9b0325a87e8edda8db560bfe287e44df79cf61edba3b2c95e34629638ecb86584f05a303603065e63323523f6ccc5b605679d1722cde5561f89d268d5f8db8e6bdffda4839c4a04982e8314da78e89f8f8ad9c0fee86332906bf78d2f20afcaabdc282008c6d09df2bfe9be2c9027bb49268b8be8936be39fa8b1ae03":128:"51e1f19a7dea5cfe9b9ca9d09096c3e7":"FAIL":0

AES-GCM NIST Validation (AES-192,128,0,1024,128) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"c6a98102af3d875bcdebe594661d3a6b376970c02b11d019":"":"bea8cd85a28a2c05bf7406b8eef1efcc":"f2f80e2c042092cc7240b598ab30fad055bce85408aa0f8cefaf8a7204f0e2acb87c78f46a5867b1f1c19461cbf5ed5d2ca21c96a63fb1f42f10f394952e63520795c56df77d6a04cb5ad006ee865a47dc2349a814a630b3d4c4e0fd149f51e8fa846656ea569fd29a1ebafc061446eb80ec182f833f1f6d9083545abf52fa4c":128:"04b80f25ae9d07f5fd8220263ac3f2f7":"":0

AES-GCM
NIST Validation (AES-192,128,0,1024,128) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"ec3cc45a22fdc7cc79ed658d9e9dbc138dcc7d6e795cba1a":"":"b10d9c70205e142704f9d1f74caee0f6":"714994017c169c574aaff2f8bad15f8fa6a385117f5405f74846eca873ca4a8f4876adf704f2fcaff2dfa75c17afefd08a4707292debc6d9fafda6244ca509bc52b0c6b70f09b14c0d7c667583c091d4064e241ba1f82dd43dc3ea4b8922be65faf5583f6b21ff5b22d3632eb4a426675648250e4b3e37c688d6129b954ef6a8":128:"d22407fd3ae1921d1b380461d2e60210":"":0

AES-GCM NIST Validation (AES-192,128,0,1024,120) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"5a32ebc7a2338038ced36d2b85cbc6c45cca9845a7c5aa99":"":"9afe0882e418c9af205eeb90e131d212":"61ff8a8bc22803f17e8e9f01aff865bc7d3083ff413ce392a989e46ebed5114894de906f7d36439024d8f2e69cc815ac043fff2f75169f6c9aa9761ff32d10a1353213ac756cb84bd3613f8261ef390e1d00c3a8fb82764b0cda4e0049219e87d2e92c38f78ffac242391f838a248f608bb2b56b31bbb453d1098e99d079ea1b":120:"fcbb932ddb0128df78a71971c52838":"FAIL":0

AES-GCM

NIST Validation (AES-192,128,0,1024,120) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"9bf22885e7f13bcc63bb0a2ca90c20e5c86001f05edf85d8":"":"99dec21f4781284722b5074ea567c171":"9f4176dacf26e27aa0e669cd4d44bca41f83468c70b54c745a601408a214bf876941ae2ae4d26929113f5de2e7d15a7bb656541292137bf2129fdc31f06f070e3cfaf0a7b30d93d8d3c76a981d75cd0ffa0bcacb34597d5be1a055c35eefeddc07ee098603e48ad88eb7a2ec19c1aefc5c7be9a237797397aa27590d5261f67a":120:"18fd1feec5e3bbf0985312dd6100d1":"FAIL":0

AES-GCM NIST Validation (AES-192,128,0,1024,120) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"cfd75a9d3788d965895553ab5fb7a8ff0aa383b7594850a6":"":"a6df69e5f77f4d99d5318c45c87451b2":"041aeb2fa0f7df027cd7709a992e041179d499f5dbccd389035bf7e514a38b5f8368379d2d7b5015d4fa6fadfd7c75abd2d855f5ea4220315fad2c2d435d910253bf76f252a21c57fe74f7247dac32f4276d793d30d48dd61d0e14a4b7f07a56c94d3799d04324dfb2b27a22a5077e280422d4f014f253d138e74c9ac3428a7b":120:"fd78b9956e4e4522605db410f97e84":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,0,1024,112) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"b0b21ae138485591c6bef7b3d5a0aa0e9762c30a50e4bba2":"":"56dc980e1cba1bc2e3b4a0733d7897ca":"a38458e5cc71f22f6f5880dc018c5777c0e6c8a1301e7d0300c02c976423c2b65f522db4a90401035346d855c892cbf27092c81b969e99cb2b6198e450a95c547bb0145652c9720aaf72a975e4cb5124b483a42f84b5cd022367802c5f167a7dfc885c1f983bb4525a88c8257df3067b6d36d2dbf6323df80c3eaeffc2d176a5":112:"b11f5c0e8cb6fea1a170c9342437":"":0

AES-GCM NIST Validation (AES-192,128,0,1024,112) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"8775665aba345b1c3e626128b5afa3d0da8f4d36b8cf1ca6":"":"cd17f761670e1f104f8ea4fb0cec7166":"2ee08a51ceaca1dbbb3ee09b72f57427fd34bd95da5b4c0933cbb0fc2f7270cffd3476aa05deeb892a7e6a8a3407e61f8631d1a00e47d46efb918393ee5099df7d65c12ab8c9640bfcb3a6cce00c3243d0b3f316f0822cfeae05ee67b419393cc81846b60c42aeb5c53f0ede1280dc36aa8ef59addd10668dd61557ce760c544":112:"6cdf60e62c91a6a944fa80da1854":"":0

AES-GCM
NIST Validation (AES-192,128,0,1024,112) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"cc9922299b47725952f06272168b728218d2443028d81597":"":"9b2f1a40717afcdbb6a95d6e335c9e4d":"bcfca8420bc7b9df0290d8c1bcf4e3e66d3a4be1c947af82dd541336e44e2c4fa7c6b456980b174948de30b694232b03f8eb990f849b5f57762886b449671e4f0b5e7a173f12910393bdf5c162163584c774ad3bba39794767a4cc45f4a582d307503960454631cdf551e528a863f2e014b1fca4955a78bd545dec831e4d71c7":112:"dd515e5a8b41ecc441443a749b31":"":0

AES-GCM NIST Validation (AES-192,128,0,1024,104) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"5a27d718f21c5cbdc52a745b931bc77bd1afa8b1231f8815":"":"59661051912fba45023aef4e6f9380a5":"2b7ce5cea81300ed23501493310f1316581ef8a50e37eaadd4bb5f527add6deb09e7dcc67652e44ac889b48726d8c0ae80e2b3a89dd34232eb1da32f7f4fcd5bf8e920d286db8604f23ab06eab3e6f99beb55fe3725107e9d67a491cdada1580717bbf64c28799c9ab67922da9194747f32fd84197070a86838d1c9ebae37

9b7":104:"f33e8f42b58f45a0456f83a13e":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,0,1024,104) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"b83e933cf54ac58f8c7e5ed18e4ed2213059158ed9cb2c30
":"":"8710af55dd79da45a4b24f6e972bc60a":"b7a428bc68696cee06f2f8b43f63b47914e29f04a4a40c0eec6193a9a24
bbe012d68bea5573382dd579beeb0565b0e0334cce6724997138b198fce8325f07069d6890ac4c052e127aa6e70a6248
e6536d1d3c6ac60d8cd14d9a45200f6540305f882df5fca2cac48278f94fe502b5abe2992fa2719b0ce98b7ef1b5582e01
51c":104:"380128ad7f35be87a17c9590fa":"FAIL":0

AES-GCM NIST Validation (AES-192,128,0,1024,104) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"d2f85f92092385f15da43a086cff64c7448b4ee5a83ed72e"
:"":"9026dfd09e4553cd51c4c13ce70830de":"3c8de64c14df73c1b470a9d8aa693af96e487d548d03a92ce59c0baec85
76129945c722586a66f03deb5029cbda029fb22d355952c3dadfdede20b63f4221f27c8e5d710e2b335c2d9a9b7ca8995
97a03c41ee6508e40a6d74814441ac3acb64a20f48a61e8a18f4bbcbd3e7e59bb3cd2be405afd6ac80d47ce6496c4b9b2
94c":104:"e9e5beea7d39c9250347a2a33d":"":0

AES-GCM
NIST Validation (AES-192,128,0,1024,96) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"de7df44ce007c99f7baad6a6955195f14e60999ed9818707
":"":"4d209e414965fe99636c1c6493bba3a3":"da3bc6bdd414a1e07e00981cf9199371192a1fb2eaae20f7091e5fe536
8e26d61b981f7f1d29f1a9085ad2789d101155a980de98d961c093941502268adb70537ad9783e6c7d5157c939f59b8a
d474c3d7fc1fcc91165cdf8dd9d6ec70d6400086d564b68ebead0d03ebd3aa66ded555692b8de0baf43bc0ddef42e3a9e
b34ab":96:"24483a57c20826a709b7d10a":"FAIL":0

AES-GCM NIST Validation (AES-192,128,0,1024,96) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"1dfa5ff20046c775b5e768c2bd9775066ae766345b7befc3
":"":"2d49409b869b8b9fc5b67767979ca8cd":"e35d34478b228bc903ea2423697e603cc077967d7cfb062e95bc11d89
fbe0a1f1d4569f89b2a7047300c1f5131d91564ec9bce014d18ba605a1c1e4e15e3e5c18413b8b59cbb25ab8f08888522
5de1235c16c7d9a8d06a23cb0b38fd1d5c6c19617fe08fd6bf01c965ed593149a1c6295435e98463e4f03a511d1a7e82c
11f01":96:"23012503febbf26dc2d872dc":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,0,1024,96) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"2df3ee3a6484c48fdd0d37bab443228c7d873c984529dfb4
":"":"dc6aeb41415c115d66443fbd7acdfc8f":"eafc6007fafb461d3b151bdff459e56dd09b7b48b93ea730c85e5424f76
2b4a9080de44497a7c56dd7855628ffc61c7b4faeb7d6f413d464fe5ec6401f3028427ae3e62db3ff39cd0f5333a664d35
05ff42caa8899b96a92ec01934d4b59556feb9055e8dfb81f55e60135345bfce3e4199bfcdb3ce42523e7d24be2a04cdb6
7":96:"e8e80bf6e5c4a55e7964f455":"FAIL":0

AES-GCM NIST Validation (AES-192,128,0,1024,64) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"ce0787f65e6c24a1c444c35dcd38195197530aa20f1f6f3b

":"":"55300431b1eaac0375681d7821e1eb7a":"84a699a34a1e597061ef95e8ec3c21b592e9236ddb98c68d7e05f1e709937b48ec34a4b88d99708d133a2cc33f5cf6819d5e7b82888e49faa5d54147d36c9e486630aa68fef88d55537119db1d57df0402f56e219f7ece7b4bb5f996dbe1c664a75174c880a00b0f2a56e35d17b69c550921961505afabf4bfd66cf04dc596d1":64:"74264163131d16ac":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,0,1024,64) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"3a15541b5857a668dc9899b2e198d2416e83bac13282ca46":"":"89bf8ab0cea6f59616eeb9b314d7c333":"4d2843f34f9ea13a1ac521479457005178bcf8b2ebeaeb09097ea4471da9f6cc60a532bcda1c18cab822af541de3b87de606999e994ace3951f58a02de0d6620c9ae04549326da449a3e90364a17b90b6b17debc0f454bb0e7e98aef56a1caccf8c91614d1616db30fc8223dbcd8e77bf55d8253efe034fd66f7191e0303c52f":64:"8f4877806daff10e":"FAIL":0

AES-GCM NIST Validation (AES-192,128,0,1024,64) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"b61cdfd19c136ee2acbe09b7993a4683a713427518f8e559":"":"4066118061c904ed1e866d4f31d11234":"153c075ecdd184fd8a0fca25cae8f720201361ef84f3c638b148ca32c51d091a0e394236d0b51c1d2ee601914120c56dfea1289af470dbc9ef462ec5f974e455e6a83e215a2c8e27c0c5b5b45b662b7f58635a29866e8f76ab41ee628c12a24ab4d5f7954665c3e4a3a346739f20393fc5700ec79d2e3c2722c3fb3c77305337":64:"4eff7227b42f9a7d":"":0

AES-GCM
NIST Validation (AES-192,128,0,1024,32) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"ce175a7df7e429fcc233540e6b8524323e91f40f592ba144":"":"c34484b4857b93e309df8e1a0e1ec9a3":"ce8d8775f047b543a6cc0d9ef9bc0db5ac5d610dc3ff6e12e0ad7cd3a399ebb762331e3c1101a189b3433a7ff4cd880a0639d2581b71e398dd982f55a11bf0f4e6ee95bacd897e8ec34649e1c256ee6ccecb33e36c76927cc5124bc2962713ad44cbd435ae3c1143796d3037fa1d659e5dad7ebf3c8cbdb5b619113d7ce8c483":32:"ff355f10":"":0

AES-GCM NIST Validation (AES-192,128,0,1024,32) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"5f659ed236ba60494e9bf1ee2cb40edcf3f25a2bac2e5bc5":"":"ad49f12f202320255406c2f40e55b034":"6da62892f436dfe9790e72d26f4858ca156d1d655c9cc4336fcf282b0f3f0b201e47f799c3019109af89ef5fd48a4811980930e82cd95f86b1995d977c847bbb06ecdcc98b1aae100b23c9c2f0dcf317a1fb36f14e90e396e6c0c594bcc0dc5f3ebf86ce7ecd4b06d1c43202734d53f55751a6e6bbda982104102af240def4eb":32:"cb4d8c1d":"":0

AES-GCM
NIST Validation (AES-192,128,0,1024,32) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"a73f318b1e298ba4ac0ab2aed74f73543b1017cccbd1b240":"":"abe33b7e8d88bd30deb96d1e90c4e951":"6de616b000047b14b6759015183dd753c61499c0e665d06a89e4fb0cd0dd3064ff8651582e901ef5d0cdf3344c29c70c3aabc2aaf83cb3f284c6fe4104906d389b027e7d9ca60d010f06ef8cd9e55db2483d06552ddbe3fc43b24c55085cd998eae3edec36673445bf626e933c15b6af08ea21cbace4720b0b68fe1a374877d5":32:"4a28ec97":"FAIL":0

AES-GCM NIST Validation (AES-192,128,1024,0,128) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"73d5be74615bc5b627eedfb95746fb5f17cbf25b500a597f":"fc40993eb8559e6b127315c03103ce31b70fc0e07a766d9eecf2e4e8d973faa4afd3053c9ebef0282c9e3d2289d21b6c339748273fa1edf6d6ef5c8f1e1e9301b250297092d9ac4f4843125ea7299d5370f7f49c258eac2a58cc9df14c162604ba0801728994dc82cb625981130c3ca8cdb3391658d4e034691e62ece0a6e407":"eb16ed8de81efde2915a901f557fba95":"":128:"804056dca9f102c4a13a930c81d77eca":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,1024,0,128) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"a249135c9f2f5a8b1af66442a4d4e101771a918ef8acee05":"c62b39b937edbdc9b644321d5d284e62eaa4154010c7a3208c1ef4706fba90223da04b2f686a28b975eff17386598ba77e212855692f384782c1f3c00be011e466e145f6f8b65c458e41409e01a019b290773992e19334ffaca544e28fc9044a5e86bcd2fa5ad2e76f2be3f014d8c387456a8fcfded3ae4d1194d0e3e53a2031":"80b6e48fe4a3b08d40c1636b25dfd2c4":"":128:"951c1c89b6d95661630d739dd9120a73":"b865f8dd64a6f51a500bcfc8cadbc9e9f5d54d2d27d815ecfe3d5731e1b230c587b46958c6187e41b52ff187a14d26aa41c5f9909a3b77859429232e5bd6c6dc22cf5590402476d033a32682e8ab8dc7ed0b089c5ab20ab9a8c5d6a3be9ea7aa56c9d3ab08de4a4a019abb447db448062f16a533d416951a8ff6f13ed5608f77":0

AES-GCM
NIST Validation (AES-192,128,1024,0,128) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"fa832a4b37dcb3c0879a771bb8ae734f0d88b9be497797a8":"0f1105f9ec24121232b60b6ef3c3e8ca9eec1a3d7625004b857d1d77f292b6ec065d92f5bb97e0dc2fdfdf823a5db275109a9472690caea04730e4bd732c33548718e9f7658bbf3e30b8d07790cd540c5754486ed8e4d6920cefaeb1c182c4d67ebed0d205ba0bd9441a599d55e45094b380f3478bcfca9646a0d7aa18d08e52":"70835abab9f945c84ef4e97cdcf2a694":"":128:"a459be0b349f6e8392c2a86edd8a9da5":"FAIL":0

AES-GCM NIST Validation (AES-192,128,1024,0,120) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"dda216287910d1f5c0a312f63c243612388bc510cb76c5ba":"d6617d583344d4fe472099d2a688297857215a3e31b47d1bf355ccfe9cf2398a3eba362c670c88f8c7162903275dfd4761d095900bd97eba72200d4045d72bd239bda156829c36b38b1ff5e4230125e5695f623e129829721e889da235bb7d4b9da07cce8c3ceb96964fd2f9dd1ff0997e1a3e253a688ceb1bfec76a7c567266":"7f770140df5b8678bc9c4b962b8c9034":"":120:"9823e3242b3f890c6a456f1837e039":"b4910277224025f58a5d0f37385b03fcd488dfef7580eb5c270c10bd7a6f6d9c7ddc2d1368d68d4e04f90e3df029ed028432a09f710be1610b2a75bd05f31bae83920573929573affd0eb03c63e0cec7a027deab792f43ee6307fd3c5078d43d5b1407ac023824d41c9437d66eeec172488f28d700aa4b54931aad7cd458456f":0

AES-GCM
NIST Validation (AES-192,128,1024,0,120) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"c5afa1e61d4594b1c2fa637f64f18dd557e4df3255b47f24":"5c772cdf19571cd51d71fc166d33a0b892fbca4eae36ab0ac94e6164d51acb2d4e60d4f3a19c3757a93960e7fd90b9a6cdf98bdf259b370ed6c7ef8cb96dba7e3a875e6e7fe6abc76aabad30c8743b3e47c8de5d604c748eeb16806c2e75180a96af7741904eca61769d39e943eb4c4c25f2afd68e9472043de2bb03e9edae20":"151fd3ba32f5bde72adce6291bcf63ea":"":120:"f0626cc07f2ed1a7570386a4110fc1":"FAIL":0

AES-GCM
 NIST Validation (AES-192,128,1024,0,120) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"febd4ff0fedd9f16bccb62380d59cd41b8eff1834347d8fa":
"dc971c8f65ece2ea4130afd4db38fc657c085ea19c76fef50f5bd0f8dd364cc22471c2fa36be8cde78529f58a78888e9de
10961760a01af005e42fc5b03e6f64962e6b18eaedea979d33d1b06e2038b1aad8993e5b20cae6cc93f3f7cf2ad658fbba
633d74f21a2003dded5f5dda3b46ed7424845c11bab439fbb987f0be09f8":"743699d3759781e82a3d21c7cd7991c8":"
":120:"1da347f9b6341049e63140395ad445":"FAIL":0

AES-GCM NIST Validation (AES-192,128,1024,0,112) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"d280d079110c1c826cc77f490d807dd8d508eb579a160c4
9":"a286d19610a990d64f3accd329fc005d468465a98cfa2f3606c6d0fbeb9732879bad3ca8094322a334a43155baed02
d8e13a2fbf259d80066c6f418a1a74b23e0f6238f505b2b3dc906ffcb4910ce6c878b595bb4e5f8f3e2ede912b38dbafdf4
659a93b056a1a67cb0ec1dbf00d93223f3b20b3f64a157105c5445b61628abf":"85b241d516b94759c9ef975f557bccea
":"":112:"bbf289df539f78c3a912b141da3a":"b9286ab91645c20de040a805020fed53c612d493a8ce9c71649ae16bd5
0eab6fb7f3a9180e1651d5413aa542608d7ecbf9fc7378c0bef4d439bc35434b6cf803976b8783aecc83a91e95cea72c2a
26a883b710252e0c2a6baa115739a0692c85f6d34ff06234fbdc79b8c4a8ea0a7056fb48c18f73aaf5084868abb0dfaa28
7d":0

AES-GCM
 NIST Validation (AES-192,128,1024,0,112) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"5e80f87fa2156c62df7be2ad16c4890de5ee5868a684fcf9"
:"c829073efd5c5150d2b7e2cdaeff979830d1aa983c747724ade6472c647a6e8e5033046e0359ea62fc26b4c95bccb3ac
416fdf54e95815c35bf86d3fdd7856abbb618fe8fcd35a9295114926a0c9df92317d44ba1885a0c67c10b9ba24b8b2f3a
464308c5578932247bf9c79d939aa3576376d2d6b4f14a378ab775531fe8abf":"9769f71c76b5b6c60462a845d2c123a
d":"":112:"394b6c631a69be3ed8c90770f3d4":"f886bd92ca9d73a52e626b0c63a3daa138faaacf7809086d04f5c0c899
362aa22e25d8659653b59c3103668461d9785bb425c6c1026ad9c924271cec9f27a9b341f708ca86f1d82a77aae88b25
da9061b78b97276f3216720352629bd1a27ebf890da6f42d8c63d68342a93c382442d49dd4b62219504785cee89dffdc
36f868":0

AES-GCM
 NIST Validation (AES-192,128,1024,0,112) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"d8a7b99e53f5e5b197364d4516cace4b928de50e571315e
3":"d0db0ac5e14bf03729125f3137d4854b4d8ce2d264f8646da17402bdad7034c0d84d7a80f107eb202aeadbfdf0639
04ae9793c6ae91ee8bcc0fc0674d8111f6aea6607633f92e4be3cfbb64418101db8b0a9225c83e60ffcf7a7f71f77149a13
f8c5227cd92855241e11ee363062a893a76ac282fb47b523b306cd8235cd81c2":"4b12c6701534098e23e1b4659f684d
6f":"":112:"729b31c65d8699c93d741caac8e3":"FAIL":0

AES-GCM NIST Validation (AES-192,128,1024,0,104) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"c874b427b7181b0c90b887147c36f242827149324fd5c94
5":"bdd90190d587a564af022f06c8bd1a68735b6f18f04113fdcec24c6027aaf0271b183336fb713d247a173d9e095dae
6e9badb0ab069712302875406f14320151fd43b90a3d6f35cc856636b1a6f98afc797cb5259567e2e9b7ce62d7b3370b
5ee852722faf740edf815b3af460cdd7de90ca6ab6cd173844216c064b16ea3696":"4b8dda046a5b7c46abeeca2f2f9bca

f8":"":104:"fe1e427bcb15ce026413a0da87":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,1024,0,104) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"56543cd6e2ebb1e3dc136a826bfc37eddb12f7a26430a1b4":"d541dd3acec2da042e6ea26fb90ff9a3861191926423b6dc99c5110b3bf150b362017159d0b85ffea397106a0d8299ec22791cb06103cd44036eed0d6d9f953724fb003068b3c3d97da129c28d97f09e6300cbea06ba66f410ca61c3311ce334c55f077c37acb3b7129c481748f79c958bc3bbeb2d3ff445ad361ed4bbc79f0a":"927ce8a596ed28c85d9cb8e688a829e6":"":104:"3a98f471112a8a646460e8efd0":"a602d61e7a35cbe0e463119bb66fd4bb6c75d1fe0b211b9d6a0a6e9e84b0794282318f0d33ec053f2cfba1623e865681affeaf29f3da3113995e87d51a5ab4872bb05b5be8ef2b14dfc3df5a48cbc9b10853a708ee4886a7390e8e4d286740a0dd41c025c8d72eda3f73f3cec5c33d5e50b643afd7691213cccccc2c41b9bd7a":0

AES-GCM NIST Validation (AES-192,128,1024,0,104) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"caaf81cd380f3af7885ef0d6196a1688c9372c5850dc5b0b":"6f269929b92c6281e00672eaec183f187b2ddecc11c9045319521d245b595ab154dd50f045a660c4d53ae07d1b7a7fd6b21da10976eb5ffcddda08c1e9075a3b4d785faa003b4dd243f379e0654740b466704d9173bc43292ae0e279a903a955ce33b299bf2842b3461f7c9a2bd311f3e87254b5413d372ec543d6efa237b95a":"508c55f1726896f5b9f0a7024fe2fad0":"":104:"3b8026268caf599ee677ecfd70":"c4a96fb08d7c2eebd17046172b98569bc2441929fc0d6876aa1f389b80c05e2ede74dc6f8c3896a2ccf518e1b375ee75e4967f7cca21fa81ee176f8fb8753381ce03b2df873897131adc62a0cbebf718c8e0bb8eeed3104535f17a9c706d178d95a1b232e9dac31f2d1bdb3a1b098f3056f0e3d18be36bd746675779c0f80a10":0

AES-GCM
NIST Validation (AES-192,128,1024,0,96) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"2fc9d9ac8469cfc718add2b03a4d8c8dcc2eeca08e5ff7bc":"bc84d8a962a9cfd179d242788473d980d177abd0af9edccb14c6dc41535439a1768978158eeed99466574ea820dbedea68c819ffd9f9915ca8392c2e03049d7198baeca1d3491fe2345e64c1012aff03985b86c831ad516d4f5eb538109fff25383c7b0fa6b940ae19b0987d8c3e4a37ccbbd2034633c1eb0df1e9ddf3a8239e":"b2a7c0d52fc60bacc3d1a94f33087095":"":96:"0a7a36ec128d0deb60869893":"fc3cd6486dfe944f7cb035787573a554f4fe010c15bd08d6b09f73066f6f272ff84474f3845337b6e429c947d419c511c2945ffb181492c5465940cef85077e8a6a272a07e310a2f3808f11be03d96162913c613d9c3f25c3893c2bd2a58a619a9757fd16cc20c1308f2140557330379f07dbfd8979b26b075977805f1885acc":0

AES-GCM
NIST Validation (AES-192,128,1024,0,96) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"81ff729efa4a9aa2eccc37c5f846235b53d3b93c79c709c8":"3992ad29eeb97d17bd5c0f04d8589903ee23ccb2b1adc2992a48a2eb62c2644c0df53b4afe4ace60dc5ec249c0c083473ebac3323539a575c14fa74c8381d1ac90cb501240f96d1779b287f7d8ba8775281d453aae37c803185f2711d21f5c00eb45cad37587ed196d1633f1eb0b33abef337447d03ec09c0e3f7fd32e8c69f0":"1bd17f04d1dc2e447b41665952ad9031":"":96:"01b0a815dc6da3e32851e1fb":"FAIL":0

AES-GCM NIST Validation (AES-192,128,1024,0,96) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"068500e8d4f8d4af9035cdaa8e005a648352e8f28bdafc8a

":"98e32428d9d21c4b60e690a2ce1cf70bee90df31302d1819b7d27fd577dd990f7ffe6ba5ef117caac718cc1880b4ca9
8f72db281c9609e189307302dc2866f20be3a545a565521368a6881e2642cba63b3cf4c8b5e5a8eabeb3e8b004618b8f
77667c111e5402c5d7c66afd297c575ce5092e898d5831031d225cee668c186a1":"5ea9198b860679759357befdbb10
6b62":"":96:"d58752f66b2cb9bb2bc388eb":"2ef3a17fcdb154f60d5e80263b7301a8526d2de451ea49adb441aa25419
86b868dab24027178f48759dbe874ae7aa7b27fb19461c6678a0ba84bbcd8567ba2412a55179e15e7c1a1392730ac392
b59c51d48f8366d45b933880095800e1f36ff1ac00753f6363b0e854f494552f1f2efe028d969e6b1a8080149dd853aa6
751e":0

AES-GCM
NIST Validation (AES-192,128,1024,0,64) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"7474d9b07739001b25baf6867254994e06e54c578508232
f":"1cbab2b6e4274caa80987072914f667b887198f7aaf4574608b91b5274f5afc3eb05a457554ff5d346d460f92c068b
c626fd301d0bb15cb3726504b3d88ecd46a15077728ddc2b698a2e8c5ea5885fc534ac227b8f103d193f1977badf4f853
a0931398da01f8019a9b1ff271b3a783ff0fae6f54db425af6e3a345ba7512cbf":"3ade6c92fe2dc575c136e3fbbba5c484
":"":64:"67c25240b8e39b63":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,1024,0,64) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"d50d4c7d442d8a92d0489a96e897d50dda6fbe47ca7713e
e":"b36b4caf1d47b0d10652824bd57b603ec1c16f4720ce7d43edde8af1b9737f61b68b882566e04da50136f27d9af4c4
c57fff4c8465c8a85f0aeadc17e02709cc9ba818d9a272709e5fb65dd5612a5c5d700da399b3668a00041a51c23de616e
a3f72093d85ecbfd9dd0b5d02b541fb605dcffe81e9f45a5c0c191cc0b92ac56d":"41b37c04ab8a80f5a8d9d82a3a4447
72":"":64:"4ee54d280829e6ef":"FAIL":0

AES-GCM NIST Validation (AES-192,128,1024,0,64) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"38f3ec3ec775dac76ae484d5b6ca61c695c7beafba4606ca
":"49726b8cefc842a02f2d7bef099871f38257cc8ea096c9ac50baced6d940acb4e8baf932bec379a973a2c3a3bc49f60f
7e9eef45eafdd15bda1dd1557f068e81226af503934eb96564d14c03f0f351974c8a54fb104fb07417fe79272e4b0c0072
b9f89b770326562e4e1b14cad784a2cd1b4ae1dc43623ec451a1cae55f6f84":"9af53cf6891a749ab286f5c34238088a":
"":64:"6f6f344dd43b0d20":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,1024,0,32) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"6db4ef061513ef6690d57aef50d8011e0dd7eb4432d8237
4":"b7f9206995bc97311855ee832e2b40c41ab2d1a40d9263683c95b14dcc51c74d2de7b6198f9d4766c659e7619fe26
93a5b188fac464ccbd5e632c5fd248cedba4028a92de12ed91415077e94cfe7a60f117052dea8916dfe0a51d92c1c0392
7e93012dbacd29bbbc50ce537a8173348ca904ac86df55940e9394c2895a9fe563":"623df5a0922d1e8c883debb2e0e5
e0b1":"":32:"14f690d7":"a6414daa9be693e7ebb32480a783c54292e57feef4abbb3636bebbc3074bfc608ad55896fe9b
d5ab875e52a43f715b98f52c07fc9fa6194ea0cd8ed78404f251639069c5a313ccfc6b94fb1657153ff48f16f6e22b3c4a0
b7f88e188c90176447fe27fa7ddc2bac3d2b7edecad5f7605093ac4280b38ae6a4c040d2d4d491b42":0

AES-GCM NIST Validation (AES-192,128,1024,0,32) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"8901bec4d3c64071d8c30c720c093221e05efed71da280bf

":"7c447e700db7367260dffa42050e612eff062eb0c8a6b4fe34858800bcb8ec2f622cb5213767b5771433783e9b0fa617c9ffb7fde09845dafc16dfc0df61215c0ca1191eabf43293db6603d5285859de7ef3329f5e71201586fb0188f0840ed5b877043ca06039768c77ff8687c5cfc2fd013a0b8da48344c568fce6b39e2b19":"9265abe966cb83838d7fd9302938f49d":"":32:"6f6c38bc":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,1024,0,32) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"2c57eb763f886154d3846cc333fc8ae8b3c7c9c3705f9872":"9fe7d210221773ba4a163850bab290ba9b7bf5e825760ac940c290a1b40cd6dd5b9fb6385ae1a79d35ee7b355b34275857d5b847bef4ac7a58f6f0e9de68687807009f5dc26244935d7bcafc7aed18316ce6c375192d2a7bf0bee8a632fe4f412440292e39339b94b28281622842f88048be4640486f2b21a119658c294ce32e":"9b3781165e7ff113ecd1d83d1df2366d":"":32:"62f32d4e":"FAIL":0

AES-GCM NIST Validation (AES-192,128,1024,1024,128) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"307d31a594e54f673bea2f977835670aca4f3d45c9c376cc":"d7385a7bd0cb76e1e242fa547c474370bcc7cc7cf3e3fa37b00fe08a56383ca31d023d8c493f6d42e482b0f32e4f244dd100ea08eee6535e5bb8d27f76dbb7eead6ba8e031ccd0eaeb649edee92aeaf0f027d59efd4e39b1f34b15ceb8b592ee0f171b1773b308c0e747790b0e6ace90fc661caa5f942bdc197067f28fbe87d1":"0bdaa353c4904d32432926f27534c73c":"aa39f04559ccc2cae3d563dda831fb238b2582cb2c2bb28cff20cc20200724c8771b9805ef7464b8fc06c7b8060c6920fd2779fbc807c2292c8c1f88f8088755609a1732ff8c0b06606452b970c79997b985889404fd907c4668a0bcc11ba617175f4525523494a244da60b238468c863055f04db20ea489adf545d56c0a71d8":128:"2ddda790aae2ca427f5fb032c29673e6":"0b92262759897f4bd5624a891187eba6040d79322a2a5a60fb75c6c6a5badd117abe40c6d963931bbc72dca1a1bf1f5388030fe323b3b24bd408334b95908177fb59af57c5cc6b31825bc7097eec7fec19f9cdb41c0264fd22f71893bcf881c1510feb8057e64880f1ea2df8dc60bb300fd06b0a582f7be534e522caadc4a2c7":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,128) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"23c201968def551817f20e49b09dbb5aae0033305bef68a0":"77bc8af42d1b64ee39012df5fc33c554af32bfef6d9182804dcfe370dfc4b9d059bdbc55f6ba4eacb8e3a491d96a65360d790864ba60acf1a605f6b28a6591513ea3cfd768ff47aee242a8e9bdfac399b452231bfd59d81c9b91f8dc589ad751d8f9fdad01dd00631f0cb51cb0248332f24194b577e5571ceb5c037a6d0bcfe8":"bd2952d215aed5e915d863e7f7696b3e":"23f35fac583897519b94998084ad6d77666e13595109e874625bc6ccc6d0c7816a62d64b02e670fa664e3bb52c276b1bafbeb44e5f9cc3ae028daf1d787344482f31fce5d2800020732b381a8b11c6837f428204b7ed2f4c4810067f2d4da99987b66e6525fc6b9217a8f6933f1681b7cfa857e102f616a7c84adc2f676e3a8f":128:"bb9ba3a9ac7d63e67bd78d71dc3133b3":"17d93c921009c6b0b3ecf243d08b701422983f2dcaec9c8d7604a2d5565ed96ce5cddcb183cd5882f8d61d3202c9015d207fed16a4c1195ba712428c727601135315fc504e80c253c3a2e4a5593fc6c4a206edce1fd7104e8a888385bbb396d3cdf1eb2b2aa4d0c9e45451e99550d9cfa05aafe6e7b5319c73c33fd6f98db3c5":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,128) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"6baec0669add30acb8f678ce477a2b171f89d1f41935c491":"5712b84c4c97d75f84edd50561bc1d3f1ba451cc3b358b2403b5e528290954348cf7a235b4dc11a72ddbc503191204e98a9744d85419508c8ca76438c13305f716f1e239a6d9f6423c27217a0057aa75f6d7e2fb356e7194f271459ab5482589ea311b33e3d3845952ff4067dd2b9bcc2e8f83630b0a219e904040abd643d839":"b1472f92f552ca0d62496b8fa622

c569":"5ae64edf11b4dbc7294d3d01bc9faf310dc08a92b28e664e0a7525f938d32ef033033f1de8931f39a58df0eabc87
84423f0a6355efcff008cae62c1d8e5b7baefd360a5a2aa1b7068522faf8e437e6419be305ada05715bf21d73bd227531f
ea4bc31a6ce1662aec49f1961ee28e33ae00eb20013fd84b51cfe0d5adbdaff592":128:"29a2d607b2d2d9c96d093000b
401a94f":"beb687f062ae7f5159d07609dd58d7b81c478d180bc0b4c07ae799626ff1da2be2e0d78b2a2a1f563257f161
491a5ac500cd719da6379e30d0f6d0a7a33203381e058f487fc60989923afbee76e703c03abc73bb01bd262ff6f0ac931f
771e9b4f2980e7d8c0a9e939fa6e1094796894f2c78f453e4abe64cb285016435ef0e8":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,120)
#0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"7b882a2df81fdb9275fb05d120f32417e8ffedd07457e938
":"0aae7213da279b34d6dcf2a691b2d0333112ea22de0c3c68d47cf9f9f4ed8ad4e03d4a60ec18c3a04ac9c2abb73e102
3051029b5e8705bb69c4c50afc84deb0379db5077be1f663652f8bd8958271af2c1ac4a87e08cb526bab8a030652f2a29
af8055d0f31e35475caee27f84c156ef8642e5bfef89192f5bde3c54279ffe06":"5c064d3418b89388fb21c61d8c74d2c5
":"5bfa7113d34e00f34713cf07c386d055e889bb42d7f6c8631ffce5668e98cb19bed8820b90ecb2b35df7134f9757003
47e5514287cfef7ffa2b0ff48b1de0769b03dca6610995d67cb80052cb2e5914eb4ed43ef5861f4b9364314fde6ad2b82f
bba7fd849dfa6e46ecc12edc8cabfff28d9bd23c2bcc8ab3661c9ba4d5fee06":120:"0943abb85adee47741540900cc833
f":"FAIL":0

AES-GCM NIST Validation (AES-192,128,1024,1024,120) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"51d94d21482c00bb5bc7e7e03aa017ba58f5a23494b72c2
a":"3a9c69c1ed2340bfde1495658dbf4f54731a19b3922a1d535df8d0b2582f5e803b5891e8ad1aa256c923956dcda24
30d0c0696bce63295fb61183e040566e459338f908d23ae51f64020c1ef3d192428f23312b285fc4111d50d1add58f4a4
9008a22c90d3365230e9158cd56f9d84f079bdd673555d4dc76c74b02fa9920e7d":"fb21cd763e6f25540f8ad455deacc
df0":"019d1db5569eeff83306f65d653b01064854c1be8446cd2516336667c6557e7844fc349adea64a12dc19ac7e8e4
0b0520a48fac64571a93d669045607085ac9fa78fed99bbf644908d7763fe5f7f503947a9fe8661b7c6aef8da101acca0a
ed758ca1580eeb2f26ae3bf2de06ce8827a91a694179991a993cdf814efbcc61ca5":120:"a93bd682b57e1d1bf4af97e93
b8927":"7093f44703f2cbb3d12d9872b07a8cd44deb62dae48bc573b11a1ee1c9f3105223423fac3181c312a8a61757a
432d92719f486c21e311b840aa63cf530710c873df27fecda0956075923f1ecc39bffb862706f48bde2de15612930fc863
0d2036e9e4cfc1c69779171bd23d9e1d5de50a9e0a0de4bd82ed3efc45299980bb4cc":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,120) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"e6756470937f5d9af76f2abe6df2d0bc15ff8e39b5154071"
:"afae92bd56c426c095d76633701aa9bea5ce05490482c6c64ac24468c3e1af6e6030a6bb6649745b011c6729bde985b
9242e22105322fbb8853dcabbd00165d0b07d7b499e0238b6513bf6351eb40635a798f7e6e2d31125dda45ffe8964596
fdbff55df22d4e9025bd4f39e7c9b90e74b3ee58d6901f113900ee47a4df5afd7":"4500193711a5d817a9f48deafda3977
2":"92fa22dba0eee6b1de1ddd24713b1be44c7105df90e6e7a54dcbf19025e560eb4986ee080cf613898a1a69d5ab460a
3b8aa2723a95ac4a4af48224b011b55fb7582ae18f6746591eab2bd33d82a8dbbae3f7877e28afef9857a623530b31d81
98b2df43f903d6e48ddae0848741f9eaae7b5504c67ad13791818f3c55c9b3d1e":120:"7d9f97c97c3424c79966f5b45a
f090":"62258d60f0138c0405df4b2ec1e308b374603a9eace45932fdc2999e9e2261de8b1099473d1fc741c46c334023
aa5d9359f7ef966240aaf7e310d874b5956fd180fb1124cbeb91cf86020c78a1a0335f5f029bd34677dd2d5076482f3b3e
85808f54998f4bac8b8fa968febceec3458fb882fc0530271f144fb3e2ab8c1a6289":0

AES-GCM

NIST Validation (AES-192,128,1024,1024,112) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"30db73d46b518669c45b81bc67b93bed3d0864f7e9e8e789":"750bc1d2f91d786bb1e621192a376f552538ba8c07d50d9e10b9345f31b3e5f9d8ad7c719c03d8548a3b184b741cd06c49d7fb6fe80258d60c01c2987c337c823211cee7c1cf82077266889bc7767475e0eeabb2ef6b5a1de2089aaef77565d40a1c2c470a880c911e77a186eacca173b25970574f05c0bdcd5428b39b52af7f":"5069e2d2f82b36de8c2eb171f301135d":"ef781dce556b84188adee2b6e1d64dac2751dd8592abc6c72af7b998dfae40cbe692a4cae0b4aa2c95910e270600550fca1e83640c64efb1eb0e0a90a6fc475ae1db863a64ce9cc272f00abac8a63d48dd9f1c0a5f4586224befed05be4afae5bd92249833d565cc6b65fd8955cb8a7d7bd9f4b6a229e3881212871a52c15d1c":112:"a5100c5e9a16aedf0e1bd8604335":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,112) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"209f0478f1a62cb54c551181cbd4d24b796e95f3a06b6cb9":"66db7cc97b4a8266c0a2228e8028e38d8986e79fcbcc3caff3050fdd2de87b7ff7a6895b988b0bdb7fcc4d6e2d538dcfaad43ce2f98b6d32500f5a6e6183d84cb19157a699cdde1266d6d75a251ee1a2eb97bfe6405d50be2b17a58ba6eafaee0a023a28d568fd1c914f06041a49c79b9df9efe63d56883cbbbeaba809273d2e":"7be1768f6ffb31599eb6def7d1daa41c":"9cb49357536ebe087e1475a5387907a9e51ad1550697f13c6cc04384ec8a67dea13376bdd5e26b815c84a78f921b506b9e2086de50f849185f05ba7c3041e49e42c0673df856da109a78b8e0ce918c25836f7e781e6b16168e4e5976d27ebc83f20b7bf4beadecb9b4f17a7a0d3a3db27fc65288a754b5031a2f5a1394801e6e":112:"4d2ac05bfd4b59b15a6f70ea7cd0":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,112) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"1bfa30b315e7b908263330140fa2d66ed57104784a43cc70":"8eeee9865e23fa51dbbf197fa41776b7edbdb9381a22c935299cd959a46190788ae82f4e645b0362df89bfc00241964784bc7ef70f6f97e81687d52e552a33af20ae34a3005e0a7b85d094368d707c3c4cd3ef31c0daf3ccaa1676609ed199327f4139d0c120977e6babceed28896d2cb3129630f3ee135572dc39433057e26a":"b7081a3010b524218390ba6dd460a1ec":"8c1f42b5931d69ae351fcde7d2b4136d4898a4fa8ba62d55cef721dadf19beaabf9d1900bdf2e58ee568b808684eecbf7aa3c890f65c54b967b94484be082193b2d8393007389abaa9debbb49d727a2ac16b4dab2c8f276840e9c65a47974d9b04f2e63adf38b6aad763f0d7cdb2c3d58691adde6e51e0a85093a4c4944f5bf2":112:"4da85b8ec861dd8be54787bb83f1":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,104) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"fc47156a693e59a1dea0618c41441fe669fc65dcfb7d0726":"3e4f0a586bad532a08c8863ebba01fd25014baa907e6032ee43d4a7dfc7c3171916dcdf9faee0531f27527872ae4e127b6b9aaee93f5e74d0ab23f3874aa0e291564bc97f17085dd7d5eb9a85d9f44574e5952929eda08863b64c85dd395c91b01fe5bef66e3fa8f9ee5bf62c25d80dc84fbe002ecfd218430b26f3549f734a1":"ea1935ed014883cc427983d7962d9992":"0d85b8513becfe8c91d0f6ffb65ec31f2cf406c51c0da88893c43d1327fd8ad1f4bab2d7b5e27438d643397034a72f8666bf641b6781bc90f764db387eae6720b5723d510194570ccd773e1b3bebfc333cc099d078583e8dac60d174d332925a24a45110c8d2abe8924ea677ac74db66ea789e2838efc96c78bceaa6236c0a67":104:"8781b045a509c4239b9f44624e":"FAIL":0

AES-GCM NIST Validation (AES-192,128,1024,1024,104) #1

depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"b5fcd780a03ba80341081ef96b440c0e4348afde4d60c1d5":"6316f3beb32f6f3bf8f2ff6a2c160b432bafd3036d3eefa1e4ec204f24892e37dc4d75c7ce9a24b5c49fb4df901f35ef9d5955f7dc289c56cb74753f4d6b2982267d5269d12237e21202a65061849c65e90e6702dda03a35ace3a3a098d16b4bfbb85b7232404baee37776a9b51af6b3059a5f170f4ebe4ecf11061ca3c1f1f3":"ad20cce056e74ec5d0a76d6280998f15":"28f8fcf23b9c1ba40c19ffc1092632e35f234c1e8b82bcd5309d37bf849a2ce401413d1f242cf255ed597f9a93a1d6e50676997f95aa612e580d88234a86ddc404292746f0b2f5cf15abebcea6659f998ec6a1cb5a9914fee5aa1aa5d04b3c20914e45095e4141ce9c173653dd91c3ebe4ed4a9a28f3915d7b2edba34c2a58d8":104:"2ad4520ddc3b907414d934cc1d":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,104) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"4382507dddccf1385fc831da8924147563416d0656e168ec":"e5c5430b960aa35dc8540215c2772d66811270859e33dd4477904759e7e5eb2986a52a4ccc9f592e614147b5ea2ead6636a15c6426336b2995d9a31ab36d76578c3540bc6693842a4bc0491c7963ee9cda2317951cf93244bd30bcdfec69a4767004636fe7d1be7300c35e80627bab9236a075a803e9e1080b9159060c643a78":"a37687c9cd4bdc1ead4e6b8f78bee7f5":"fa9ae30509cbb6fe104c21480ae7b8ec9f12f1afb17320d77b77cdf32ce8c5a3f7f927e501118c7ccd6975b79225059cef530a4fcb0a9719f5e2d3bebe7bb6ec0855e495a31e5075eb50aa6c1227e48b03e3fdf780084ac4912eb3a5674cca9dd6ac037366b230ae631a8580d2d117942dee5d5ddbbb2233afeca53289cc4f68":104:"4221818d4be45306e205813789":"b5b36719bc4d13a5fbf37188ea814cdf3c97a430784330540325c899570e15482300bc82c5b8163074e0544c5132e3ce93bba68bd7a8d2db81d1431b424b697c1158c4d70625666d5ff99145ca34856815c905b5a0fd95806df56b9cd5b384bda3e394b409048eb1037144cc071539c02397e931da28a43cc354d584643afd4f":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,96) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"7a66db3450dac9a1e63d2639f34c5c6a3fbfb3c8e8230199":"6463a7eb2496379bc8a5635541525926a6f9fa718e338221952118ae4cf03a85f2074b4ebaf108b9c725809be1e6309c3a444b66f12286f6ea9d80c3413706b234b26372e8f00783819314a994c9e3ecf6abdd255cbfe01b3865e1390a35dcd2853a3d99ed992e82ec67ba245f088cb090adade74bdbc8a1bad0f06cbea766a6":"21f8341529b210ade7f2c6055e13007a":"1699bc8c198ab03e22d9bc4f3682aad335c6e35f3f616bb69769a9d5a202511797e770ae0d8d8528ef7b2bb25b4294d47427b43f0580fa71d93fdef667f4f4196f84e41c0b1978796d0de74a94420fb8571bff39137fa231c572b31be9ae72338288bef5f8c992121dc918538551f346e279a9047df14ec9fc0fd399cd3bd8d8":96:"4af02b81b26104d1d31e295a":"53fe6a34d280f2c96d1ae2b2e8baf6abd67cedf7d214312f75dd4a1bec28a641dda3e71aa398726b2b0b1f515e1f4259ee97acaf17f122db9ec7814c2de6a88d36c3ac106396ad03d337c2cd2d2b9b4b7170e23a5848ca7ea129838f967dfdfe83b45ff2a9be699bfb2346115465d59f074f09e24d8fcbd9ece0018c92776c43":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,96) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"1f5c818f24d201f9fb23fcca211b0545eee5c5c9b440810d":"9a7566817a06f792e96a6a2ba8e0a01f8837e2de06796e68b0782cc54ed0b04fc5e24a1ad37d5ffb035548b882d88150e89915b89f57cde2bf3c43ab9dae356927daef6bd61cc9edd5e1b7a4abea2f71313677f1b2fdf3d8d4a7e9814ea820fbc3e5c83947db961839a985a57ced7f5e4a1efffcfd17a2c806d4cdc1e79162da":"3a163067bdd90fce0406d1c198a88771":"a5e94e233d04fe0c4b6c4684b386902fe05096702237dfbe76f73befa69b6f30394cf9fe3358997942df65842748fb4f075a3dc06e147bd8d67fc4371113a4d75c70219257c650a6f38a136659e20a1cf3a119397835c304e0fb2a33aa3c3019175c86463043d5edc6992874f61e81cd0d26af8b62cf8c8626901d4f16d84236":96:"b124eea927e2a62a875494a1":"FA

IL":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,96) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"9a301f7edf83da63bcf37216a3a33d7613331c3210281dd7":"e09cc8543db7804870004706a26e94b457c125bd648b581a196f962f2ae8fa55d9bc66530ba5020e22d282080b4720dc9a2096a11c0fcc3d9a67cd1cf95cd7cd2417ba308c761e64be24347a14c9423447094a5c72a0043c288b35e753ba0aa748f208381249fb1c8d195a472192404b6c8172663ee4b4d4ecfa426e1fb003f2":"d73a546b0fa307633ac89506fa86138b":"f57fe548cf4a551a216ffb24a1dcf1b79c95f9abf06443fd58af042d287c2165db373c82a94172db517840f22e45e966e3ead91ce1ddad132bcb844e406e84b76a0b5b0ee23064b66a229f32a2d3b9c71103f020c4ba57fc0f0608b7114914cf2ada0c5a9bc4afbfa9ce5da320f34beb2211d569a142f53bfd262f6d149c4350":96:"f536a3b8c333b1aa520d6440":"124a327a8c22b7652886dac2c84b8997ca8a6f61c9ba9c094b5aea41eaa050a6df6cbf280259e5466071bcfa53b4ebc76c3cc4afc8c0385189a5382933aa57c89aab78dca84331e0fe8f0aab3a7857d3e13f08dcd90ec5f0684f82088ef8eb7fd67e75de43b67afc3a0beb458f5ebd61b2c779e6c539d795c667bb7dcc2b762e":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,64) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"fd40e8226fd13cb95ba50b7cdf0f07f7ab7037cf8705ca50":"75aa7df5c3c443d48ee998064b6fd112c20d2d90c98e00d025ef08d1ad3595385be99de47fa627549b827c48bc79eb1dcaf2f1be95a45f7e55755b952aee5ae0748e68bee1b014a628f3f7dc88e0ebac1d1d00e268355f5101838ce125c57003aebc02a1c9d6ae2cd6e2592f52c0be38cef21a680ae35c909cab99dce9837aef":"3406e70cbe16b047fedaa537eb892279":"390b18d22d5ecc0b5a524ae9afac6fd948ac72d1360775a88b385aa862cce8a27f3e4b420e539bec6e8958f8c1b5416c313fa0a16f921149a2bfeae29ad2348949b29a73970e5be925ec0c35218b82a020cf21bb68c6931f86b29e01b85500a73f3ee7eb78da60078f42550da83b2e301d151d69b273a050f89e57dfc4787cbf":64:"69e06c72ead69501":"6e8d661cd320b1b39f8494836fcf738b0ab82873d3903c9ee34d74f618aea36099926b54c1589225ec9a9d48ca53657f10d9289c31f199c37c48fb9cbe1cda1e790aaeedf73871f66a3761625cca3c4f642bc4f254868f6b903e80ceeeb015569ace23376567d3712ad16d1289dc504f15d9b2751b23e7722b9e6d8e0827859f":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,64) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"a85ab87563b809b01725764d64ba4cc6a143e2e0362f0c52":"ef43629721b50bd3656b7ae31b6e4b4ba1cf2c72ed0460ee7d9fb416631ddc597e5f9aebbcf4442b95cc46e28476a464dd87caf9c1c1d6c99d3e3e059dc23f8d2fe155ff5e59c50d640bc052c62adee3aa1295b38732e3458f379e98a8dbdfed04c22a5761792e87fa67ecbcbf3b90eb1bcd1d3f49e60132452f28afece83e90":"9f991ff16a3e3eb164a4f819c9f1821a":"df289511f78d8fa2505afc4c71ab1d7c31a8d15d1e5fcbb29d70f0e56f89c4d7b30f1b3b4745b5d2cc7af34fb4c95461372bf516ec192b400dc8fdb0ca9fe1f30f5320d0fadf20155cfcddcf09233c6f591c1c89917e38a003f56b94a1e2429d1f2b6297db790d7dce84d9fa13d2d86a0e4d100e154050b07178bee4cdf18126":64:"dc4c97fe8cc53350":"ff0e531c7344f0425d62d5fbedf4bc8d3d5cc80647e67b852c1a58ad1516d376d954cb8dda739f6a4df3cf1507e59696610bcb6b34340d6313028e00d7197845d392e73331aaf168b474a67364d8f9dab740509fabf92af75045f0afabc1b5829264d138820952bbc484d1100d058a4de32b4ece82746b2b4a85fb2993d4add8":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,64) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"f4f1e03abb927ffd0b081b9dce83a56a6dd419a6313ac34f"

:"0e70421499bc4bcb3851afa34cdf5be374722815abdd9bcee5f332dbe890bdc1c0210ab10667e5bb924bf3c1120e25a
0c074da620076f143940989e222086d1b34a1200d09aea1f810ef6de7d8520c65eef9539fde5a6422606c588fce6264e5
f91f934ede6397c4b307d2d7e07a518fce577a427fa92923cbba637ae495afad":"d1e29bb51a3c4e871d15bb0cd86257e
2":"ae2911cdaaad1194c5d7868b6d8f30287105df132eb0cecca14b6e23ec7ac39cc01da1c567a0219cca7b902cc2e825
e30f9524a473eb6e1d4d1beff5ab4f29103b2c7522a33dd33182fa955c4f09a75196b1072a6f0340fc55a802d29c7067f0
5219c21857ebff89ada11f648c1f28dfbfdaab56028f05509de17e2381457ebc":64:"44f760787f7bc3c0":"2199fa50514
61b67581429ab19de2ccb50b8b02e12c0e1d81a8a14929f84e09d9715b7d198e77e632de4af1c08c5041276204a7ed76
646385e288e96e1a4b0b0f2b1a9df7f0892beaea3cb58d9632720158f6daa4cbbfc0ebdc56ff6a5175768ff2abd24cb766
9bc3fe40f8aba7869d2dd7dac86b6ebc4e4ce261edbec88db17":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,32) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"33efe20433c6a1ad261a1fed494961749e5bf9d35809b59d
":"cfbeb61be50def25f513346498f75984bfe797a8ad56be34f2461e2d673f6ce14e7479a59777267b75dadc6b9522599
ebe5d7b079495a58ca187ec47796f6ee8c322278ad7451b038c938928adcff6105a8ea3780aedc45b6a3323d3ae6fbce5
da4fb59ca5ec0a16a70494c3c4859672348532505e44f915e0b9b8a296ef5225":"dc94673b0c49c6d3b4611e278212c7
48":"919f7397a6d03836423b7cac53177fcfbe457d4aa4348646f646aae1bc5a15568cdb8c96fabef278ace248aca5311
10a4f4f9e8ab0c32525ad816ae3facf03175232dc84addcd6065f9cc1f513966b63fd27e91a09f1921b95d6bd8f08f1dbc
e073bcf827847f774514b478b9d7fb5426847dd4dee6f39b5768c1fb729b32d03":32:"c5098340":"c5e47d8c60b04df1
974b68a14095d9bc8429a413d21960b15bae4fd7356bf7872e0da0a1a385ca2982d3aa3182e63ea4bb8ca01410cd4e71
ddad34aa1f12c1387902b3d56634f89c619a2e6756648ab3bf90e9bc945afc9140eb935b633bae96bb067e9ee421697bc
f80b14b1b88dbf13e010b472a7ca5411db36848b9c7a37f":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,32) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"3ed5dadefa0f6d14fedd1a3cdbab109f6660896a952ac5ab"
:"aef617f69724e020309ec39d9587520efda68a8e303686c3a41ef700cba05b7c6e43e95aadb1a566f61650c87845835e
789eb2366941e3bfef6d9846af0e0dbc43249117ad6f299bbc40669ac383cdf79289ada6ccd8ccfe329a0dc6a38eea1a99
550457102d10f641cda50c21f533b1f981663f74a0a7c657c04d9fc6696ff4":"553a14f1e1619f9d7bd07cd823961f25":
"eb8ea81d3e328a1113942cd5efd0f2b5e7f088791c8fc05690a34584101c4d493628ee7d0099a2865ac194b9124c3fb9
24de0c4428d0a1c26ea3ad9a0bc89187a16673e3b6f7e370dfb2dc26e8a56a9cf91f9c2088c020a766efe0d0c91689743
a603f2cd1e300a6a84828b3b515a4b9a06e6bb20457bf124cd6ce4ac8b83d51":32:"dc413c4c":"bc1f34991a48aabb0fe
a513f790f0d223e9feac4c99fa1e8427f01ab8b4b2827cfaf239342de36051a846af0306a3f82e7aed98dd0416fb078bc7f
3b617b00ceb2cea4ddafc22dd022efa8303e9804510e0e888065d8427345156d823f796f74130c06db9f9934435552b4f
efd051953e20ecba3a4514ac121d7d2097d597439":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,32) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"6d97e8bff3923a778504fb917dbc1428a1328587047697d
9":"dc1a81efd51e967767f5bdd7e2e425732c1d28451f2bf5bdf3f5a6492279330594d360dd8a193e5dbde1be49bf143a
35c38bcd059f762ada65c5119e097f0976891347f4d829b087bd72daa3494b344cbd3370c4459ca243bd57aeda4cb86c
dd0bf274f07830cdbf5e5be4eb9b742ddffef8aa35626d2b9ea0a29d3c3d058b28":"0c28dc4cd53725091c2fb68a476c2
e40":"f3932f5e82d75a1e3eba1591c17769e1a45819ccf057c31e76fa810b93678766d25905e859775c244e96bcafbc75
c4a2d95e7d02868ccb2f65e49276f0b645ac8cf6e3758402304a3c25ce2de0a49f401b1acadaff8b57589b45cc79130ddc
8387f41cc383e33ef38eec019152051c756198d6f782ccf56297b9fe944269a65a":32:"e6d6df7a":"39327836e9d8cfb5

9397adcf045a85644c52c3563290795811f26350c8bce8f55ca779cbcd15479efd8144b8a39ef611153955c70bf3a7da9
d4d944c2407a0d735784fcb68de1083eebf6940ebc9cf92f9f139c01404b503ff64e61126a94e88135147350788435704
0fd32714b872c254349071069644e2bd642905521b944e":0

AES-GCM
NIST Validation (AES-192,128,0,0,128) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"2c78e29971e90a01bb65973f81260b9344fa835751f5f142
":"":"f1a23ce6e2bc9088a62c887abecd30ae":"":128:"d4d5c22f993c8c610145fcbe4e021687":"":0

AES-GCM NIST Validation (AES-192,128,0,0,128) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"8c582d5b6a40ef0e4048ec20f0263572d7cc82704e38085
1":"":"ef221a1c66fda17906190b7c99ab60b8":"":128:"6327dcb46ffb3d0fd8fbf3d2848a8f01":"":0

AES-GCM
NIST Validation (AES-192,128,0,0,128) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"3a58abadd29e946e23ca9eb09af059913d5394971bda6a4f
":"":"7c29b3196d44df78fa514a1967fcd3a6":"":128:"fc123944bbea6c5075a5f987aed9cf99":"FAIL":0

AES-GCM NIST Validation (AES-192,128,0,0,120) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"04bdde4c35c385783715d8a883640851b860ce0e8436ec1
9":"":"783f9a3c36b6d0c9fd57c15105316535":"":120:"23e21a803cac5237777014686564f2":"":0

AES-GCM NIST Validation (AES-192,128,0,0,120) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"4ba5fba0c22fbe10c2d1690c5d99938522de9c5186721bac
":"":"2acc2073089a34d4651eee39a262e8ae":"":120:"7ac742c859a02a543b50464c66dcf5":"":0

AES-GCM NIST Validation (AES-192,128,0,0,120) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"f12890b0a8819faa5a8e0e487f7f064af42fa6d5519d009f":
"":"c937615675738f4b3227c799833d1e61":"":120:"88300bd65b12dcb341f1f6d8a15584":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,0,0,112) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"51878f3630298a81297f4a21514fea637faa3815d4f26fae"
:"":"1f939226feab012dabfc2193637d15b1":"":112:"eed5fcb7607c038b354746d91c5b":"FAIL":0

AES-GCM NIST Validation (AES-192,128,0,0,112) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"ae596e74840a600556a06f97b13b89e38f67c152f1a1b930
":"":"e2076e1050070d468659885ea77e88d0":"":112:"b4586bdbd4b6b899648f2333eee0":"":0

AES-GCM NIST Validation (AES-192,128,0,0,112) #2

depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"fd33b7a0efae34339ca987b5eb8075385fd1276e63cc8530":"":"2d07bb8616fc0bbb71755a1bd256e7fb":"":112:"6b60d645220cfde42d88296ac193":"FAIL":0

AES-GCM NIST Validation (AES-192,128,0,0,104) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"5685b12a6617d554c36b62af5b8ff2239cb3ffb1d2c40e14":"":"6c31194df99d08881fa5b1dd33b45a92":"":104:"69431593c376c9f8052bf10747":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,0,0,104) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"036ae037410dae9f0741608516d03b855c9c1851df8c54a4":"":"73599275f8237f14c4a52b283c07275d":"":104:"6f7249d25c9f273434c4720275":"":0

AES-GCM NIST Validation (AES-192,128,0,0,104) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"ac144f39ebd6124bad85c9c7fb4f75bff389ece2e8085d83":"":"d0871bfc3693245be478e6a257c79efb":"":104:"5a99d59631d0e12f58b7b95ccd":"FAIL":0

AES-GCM NIST Validation (AES-192,128,0,0,96) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"a8a541ff11a1b8548e832d9e015edeccc94b87dadc156065":"":"c72bb300b624c27cded863eba56e7587":"":96:"ea2528e7439be2ed0a0d6b2a":"":0

AES-GCM NIST Validation (AES-192,128,0,0,96) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"30dd8f400335e9c688e13cc0b1007bd21736a6d395d152e2":"":"28899601fa95f532b030f11bbeb87011":"":96:"35625638589bb7f6ccdb0222":"":0

AES-GCM
NIST Validation (AES-192,128,0,0,96) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"cb8f672b04d706d7d4125d6830fff5d2ec069569bea050ce":"":"375d4134e8649367f4db9bdb07aa8594":"":96:"70610bf329683e15ecf8c79f":"FAIL":0

AES-GCM NIST Validation (AES-192,128,0,0,64) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"bf71e5b1cd6eb363ecd89a4958675a1166c10749e1ff1f44":"":"9f502fb5ac90ff5f5616dd1fa837387d":"":64:"a4b5138122e1209d":"FAIL":0

AES-GCM NIST Validation (AES-192,128,0,0,64) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"5b9d1dfb2303b66848e363793bdca0e5ada8599cb2c09e24":"":"2ee96384dd29f8a4c4a6102549a026ab":"":64:"3b33a10189338c3b":"FAIL":0

AES-GCM NIST Validation (AES-192,128,0,0,64) #2
depends_on:MBEDTLS_AES_C

gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"a35ae271f70ebacb28173b37b921f5abcad1712a1cf5d5db":"":"8d97f354564d8185b57f7727626850a0":"":64:"813d2f98a760130c":"":0

AES-GCM
NIST Validation (AES-192,128,0,0,32) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"9bdd0cb826d5d28c2ab9777d5a0c1558e7c8227c53ed4c4f":"":"daf13501a47ee73c0197d8b774eec399":"":32:"a6d108c0":"":0

AES-GCM NIST Validation (AES-192,128,0,0,32) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"81b4d5ee4e1cbee1d8966fb3946409e6e64319a4b83231f5":"":"bc2f9320d6b62eea29ebc9cf7fc9f04a":"":32:"a47cdadd":"":0

AES-GCM NIST Validation (AES-192,128,0,0,32) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"5813627d26d568dfe5a0f8184cf561fe455eb98b98841fe0":"":"817199254a912880405c9729d75ed391":"":32:"d81d9b41":"":0

AES-GCM NIST Validation (AES-192,128,0,1024,128) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"94f160e2325da2330fbe4e15910d33c2014f01ace58e5b24":"":"80a1b99750980bf2be84a17032fc2721":"066fdd980cf043a732403ee5f65c82ca81e3fc858ad3cfa343014a8426fd3806770f127e2041efb42e31506ce83390ac5d76de2fe1806df24ce6e4bb894972a107ef99e51e4acfb0e325ab053f9824514b5941ab1ec598fbb57a5d18ed34d72992a19215d914e34ad1a22326e493d1ff2da7bc271c96ad3ab66d0c32bd711293":128:"dd153cfd7aa946280660c445f586fa28":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,0,1024,128) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"4785846f7c0524e78f3eb137fd433e1808af64549af69183":"":"5334476a5fa3fa50dcc4b12f8ac00b51":"e70f82d1e3361ac5a5c9a087e47984d5533ba296f9b7e4a192a4ab28a833cdbbd5cece3415cf6fbb2f8055560b5c31c98d83d139954e1c03a464739f1eb5ad982c4371cf20b8984bbd97d5f40b336f5e96df3d272b95f7547be15c3bc05b3caac7d08c5eb5de8bdd246e74f6caa6bff76ea0417730ce72b911867f88fdcf73a0":128:"c59231ddaae98e0e8db6b3fe8f4d3427":"":0

AES-GCM NIST Validation (AES-192,128,0,1024,128) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"49b085fe1a8e1ae769ed09fc585d29eb24d589689992e6c5":"":"899878b0684fb865d30190821817b88c":"f789eafe3d02826b619ca4fbca7bb1919e5c6f7c33824a2f7f815dc50e329979705f7ef61e9adf7899d34f1b8840384ff62ef6d29eea38c45d12be9249aca69a02222cd744d81958c6816304ff0d81d6714a2023b3dd9d940db5c50afd89c52774d28d6afde2b6c68425b6acbe34682531a2e57e2b9a7729b3e8d96a729b15cc":128:"2c84bf7a8947ab93b10ae408243b4993":"":0

AES-GCM
NIST Validation (AES-192,128,0,1024,120) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"75847588760ecb6ca548747b743914c89fea367a5ccb81b

6":"":"7d8a9fd254e2061c01e39eb574951924":"b03c57dfd49152401a225357f1d6e533f3a423e5cfce07b8ae7ca9daf6
8645e5bd67b3ca2421eac447530b27c6dc6bd9c7f1b22441b8cc8c4ac26cec2c9c0d665a35b66d779a3772d714f802d6
b6272984808d0740344b6abdb63e626ef4e1ab0469da521c7908b2c95a0fd07437c0e9d4d2451ae189ad61ff19f4efb40
5127c":120:"e8aac14b53cdbc2028d330fc8d92a7":"":0

AES-GCM NIST Validation (AES-192,128,0,1024,120) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"e3a18a96d2e45d2f60780dc39cee7160e28cb810bf09858c
":"":"26a4d659665ded39b7a1583de756d0ad":"83f8d9c58169b4c68032321197077ff5c8ee4ebb732b040748e1b55dc
f53375ae86fb9646a672b5c5bc805a92c475cbb6d0ed689a58abdf2230250a7d3fbd8cfab07835fa85e738a7f74bc3e936
16d844b1ec61b79f23dfea62e1815f295d43f61d7b5956103b31ca88afb0b3d37eb42cf77232dbf2258065232971c397d
cbcb":120:"dc034564d4be7de243ff059b5f9160":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,0,1024,120) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"7be3909170ea7a2ff76f9f28241d8cc48ddeafa8517c6f8c":
"":"8dee7e29350c60c5bcfec89da6617d2e":"f6e9e7a7f9716760eb43060d5c80236a0f118b0f750ebd5df01fd2dba95c
556ecd2e54a3f337767321abf569c8137a8e48c5b44037ba62951e9f9f709e6e4540a36d769f3945d01a20a2ed1891c41
5a16d95cab7ddf9bcebf18842c830067509a2a5d49a9684324c433d53824d2f8fd326b149af17f40e5bf5e49185738fba
60":120:"942b52277e9dc0a30d737d00f5e597":"":0

AES-GCM NIST Validation (AES-192,128,0,1024,112) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"1fe413bafc4753e1511b580c830449bee56e0e5b9acb852c
":"":"e30829f64f3eda13bfb2ac572aceb3de":"6c772d08b4d7507e35804572fa697c646c77301954cc5c160941e49e23
0697ed8c23338b9f30c3ead69b1c1a2329ff025dcd3c0d0a9cc83fee4979448aa71ddb9d569bedc8c497a2a4ac3b60d08
7d7872f0a110bf90493ae7da03b0953734223156cd2d6c562e4a978a6dd5cdb229dd58dd4d0f50ac015f2f5e89dac4aa2
9a19":112:"87737873b82586bb29b406946cae":"":0

AES-GCM
NIST Validation (AES-192,128,0,1024,112) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"b4bc4378d423931f9b320bb57df584c641406c1daa7448a
d":"":"eca70e10c0358838a3f4a45c4b016ccd":"68d1c045c1604e3c3dd4f7c7543240aca8dbc5266dc18c5a8071e8b09
e3700b7cf819044b2722d8db92021f42a0afb295d7b16ecf4e4704a50a527a2e72d7f53617c358e3b7be3d7fecda612ce
6842fcfaa68f2d1b8a59d8b8391779f2fab99f820862c94029f444abe62367c5de0a4becc359660e4a5366f7d482bdc362
b866":112:"06f95ca69c222a8985887925b15e":"":0

AES-GCM NIST Validation (AES-192,128,0,1024,112) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"1cd4414ffd24e830e2dc49727efa592e430a6a75391cf111
":"":"a08e32ad7d63f975de314ad2c0fa13fc":"20a271f1f4c6bea8f1584ab39a7179ec448650e2ff67a7338d1bc9fab7f7
3b2ce5222cd07ded947d135d9d0670dc368f0a4b50ece85cbf641877f9fe0ac6a7e6afb32fdb1b3cd35360bb80cfffc34cf
b94dbcbee9ca5be98a0ca846394a135860fba57c6f0125dcb9fb8b61be681ada31a997638ee172525c03dd13171534a9
1":112:"c68842cafc50070799f7c8acd62a":"":0

AES-GCM

NIST Validation (AES-192,128,0,1024,104) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"9e0ef9ed5e6f00a721a9893e1f0d9079c5aa667a4cdd2a52":"":"5f015fd556e87ff0d0df586fb452306d":"b82986135e49e03f6f8f3ce4048ded2e63ee0c31ddc84929e022ee8561159179b3bb4403ebdafdf6beae51ac5bf4abed4dbc251433417ece3228b260eca5134e5390cba49a0b6fcbbbabb085378374e4e671d9ba265298e9864bfce256884247c36f9bddceb79b6a3e700cb3dd40088ba7bb6ab6aa11b6be261a7e5348f4a7d1":104:"ec9a79a88a164e1a6253d8312e":"FAIL":0

AES-GCM NIST Validation (AES-192,128,0,1024,104) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"9bc8f15d98e089d60d4db00808700053f78b33c31652c3e4":"":"5cc0ff9bb7d5b9b2aa06f6ecf669d5bb":"24ac95a6ed2f78853f9ab20f53de47e7f662f72aea454141e2131aace7ed2daeb395bbccdbf004e23ce04ad85909f30151b6526c1ce7934726f99997bbab27055b379e5e43b80ad546e2d1655d1adad4cbe51282643bb4df086deb1b48c1bd3ac3b53c4a406be2687174028ecf7e7976e5c7a11c9a3827813ade32baef9f15ec":104:"9779b7c3ece6c23d5813e243ec":"":0

AES-GCM
NIST Validation (AES-192,128,0,1024,104) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"19afc43a4481f796d77561f80b5b2e1514c96c5d1d86e64c":"":"d4c06595fefd4a81bbbd4b40c2e1989d":"98fcca51352998d0126b5539e3fb9a238ac31c05954fc206d381909aee70983b6ab99d3f3efe8530a1c3cfe3b62756321b1d0771a5940055eba1e71fa64f29291aa5e5b0af0fcc8e6f5a02688d9e93417225eded791a35217822ffb346d3fa2809b65abe729448316be30cf661137d3c0e49846cb0df598d90eda545afb64a5e":104:"ca82448429106009094c21d70b":"FAIL":0

AES-GCM NIST Validation (AES-192,128,0,1024,96) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"b4fc31dcfef6203fdb296cc928c13b7df56bfe6f32583057":"":"6308a78dc8f3c90442dc52196649c38e":"2567d80c253b080c0158102558551445d8ce4d5ddee2014a2be5cbad62e1717a0fd4d2059447c3151192951eb11a4a7b19a952f6ba261c87f10f4c9032028de3cc5a2a573a4e993a690fc8954daa3ec92743e7343e75b646c4fa9cbc3fceb4f5d59bb439c23754c4d9666fbc16c90c0cac91679b6ad1bfe5dcf6bd1a8a67c6b5":96:"9d1603799e2485a03e7b05a0":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,0,1024,96) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"1c2d9412486c381440213e1588b6bb58b0da53300b9d3089":"":"727ed8846daab874d5a9918b47d016f4":"656430f0c1423018b5e2efbb1e32a5385c1a9a1779c4dbd585dea91edc39ea8752ebfc2d8064251a8a5ae71e1845f24a7e42c6371c2ecb31e2229d5f4923bffc21d4804575a84836f3cf90ec6047bb360b558a41a975ece111b5284dfa2441705a6df54fc66ca6cc1af9163ecc46902fac337d5f67f563fde8e8e7e64b8588b7":96:"05ee6ce13711535864674a5b":"":0

AES-GCM NIST Validation (AES-192,128,0,1024,96) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"abf7a97569427225a4bd5143c716a22e62f84c145bb51511":"":"e255088cdfe8ae5c9fea86d74d2f1b7d":"b850993300f54d078f83ceb9aef7345bbf758f92365b6625c210f61dad4f2a2319f51d883a383a706392d3dfca1706eba585a6fac8bd4294c0bb2cb3f6b454d5c97819e8e5c926754840261b07ec4ef1f87cf281d75c187839689944230306e1903047915e086043990745864819ad713d34a244aa4e9d755fdb137105d

7eed8":96:"0c9c17388d0610f99d0a093f":"":0

AES-GCM
NIST Validation (AES-192,128,0,1024,64) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"45a6df655e88bc880acff41520aafd0cc8aa8aeb8952fd06"
:"":"1125e1de94970c9e7be70e58e7626ef4":"fe9838a445b8edef19b3e9f33c8c0c265b3a12c97b8ec57ceb94f65ae522
7177de38f1e338dccb2b24e5bd0f0eb8127f83eba0f1ddfa55198789df0cdd1d977fcb985ad9c7d51b96e749d2cf3cc7a1
ec4dfcbc641a1a022d55def328e081af890a7e699f2dbafdf506389e045aa1219239d5868ba675a3925602b6fb6f6e6d37
":64:"1c3bd1e0d4918e36":"FAIL":0

AES-GCM NIST Validation (AES-192,128,0,1024,64) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"279f4f2ab4b70778fdb9ca7800cd20e323601d7aa2c75366
":"":"0f7b402560735cf03d5da58de5b6c685":"7dd9a8c848bbcf5127161c8a419a436a0dad559f7c1613cdf41594e177
016acb1ccf44be852185c42e7120902a42efe83855995ab52cf5c190d499fcfd698c671fd72949dc3ea7ddb874e586a3aa
455a021cec7b5f8608462ca66f926aba76e60a5846d4eb204155cd3c1328da51ba35c3007b8bb394f34e3a8b81ddd2ea
1115":64:"dab612351f75e2cb":"":0

AES-GCM
NIST Validation (AES-192,128,0,1024,64) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"6716ab937755684af7403e6fba5452c1b11568a9047bb50
f":"":"2fd5a446dd564619ef75b6e00905ffe0":"20d261d3192996c21da69e979c26f5f937e6ea4cb7b05c6ef556ce4d86
ca0fe85ec2425d274c43b5212fe9d27bb48b04e887461a9f45f524059b87eaea2e287a8d4537f338b0212012a9d4b6610
e8c97dd554e0b3c3133e05c14d0ddab3524c93fd527e223b1996b4cff0a4a7438f1d54890bf573cd803941b69e5fc6212
c5d2":64:"f1d743b7e1b73af5":"FAIL":0

AES-GCM NIST Validation (AES-192,128,0,1024,32) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"7dc94b5bbd6315ad8d2b67f0c683d10cf456f822a3ebb02
4":"":"6f3eedeb57dcf12bfb3cd80849893c90":"ee1ff367f4b23c156e3dccff84ae4bf2b8ecec1fb5ffd25ccaa93b6c6834
389bd79655bd4bac75238eb0f65d3603ecc57c8774798309e85b6677e78ed2077b712cf28795d0dc8fee994f97373a82
338ef67c62378136a79a990ecbcd6367445e805efa98f9168826e57cb8dd7e7b1d5c89ad98358646fa56dd2a71c40e027
5a1":32:"4dc74971":"":0

AES-GCM
NIST Validation (AES-192,128,0,1024,32) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"3bbe223e253bf272599e28af6861013ecd0c88710947ed4
1":"":"4fbf09ffaffb600f0de38fb12315cab5":"5388146f6479f7b3b280f45655a95b847ee27c734fb2fd91f6c009b1ab1
810c772c7435d3221069f9490d251b76e740147906ac1db1c209c175b21aa10881c44fb307d4d2900aa3b1d56fb0edb9
f2a58505653a17fee350e12755b9656bc65c78c1593d5cb7178e29f82209caf53e60fddf725f6957cc9718bf410c4a0229
ed4":32:"fb845ab7":"FAIL":0

AES-GCM NIST Validation (AES-192,128,0,1024,32) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"461877813acfe6e9979eab729b52e3d192b3236758bb656

3":"":"6985cf77b75a47a3978dd6412d59200b":"385551854a89ab37063ba0ed911501b3d632153c5c2992e154c0a334bc36620476f11495437b842409e0954f7352cbf288d158bdbbaf72621ea2ce75b708bc276f796c5aa7fd0071e522c5f175a9e7787deef79f6362101aa3607b4588f2e1df7127f617c6073593a1c792b959e201e4a7a43ea8b1c3af026376439ef629266c":32:"c840d994":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,1024,0,128) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"09770f9114120a2c1c3cc416fe0eb8699e07141158a5bdff":"875e2e5b5c02e0a33e71b678aa29c15ce18ec259cf4b41874893ed3112daa56ff2a7475681b8b3d9028ef184d30658e881c908f3588f69899962074db4ddfc0597f8debb66c8388a1bccf0ffe2cf9f078dc1c93f8191f920754442ad4a325985c62de1a57a25de4e9ed5c2fd0f2c8af33f3b140bac12bf60fdb33e0ec557955b":"cff291d2364fc06a3a89e867b0e67e56":"":128:"81f1eb568d0af29680518df7378ba3e8":"FAIL":0

AES-GCM NIST Validation (AES-192,128,1024,0,128) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"4fbf1c785c087ad06b43d4163cf9b9396deffd3712856379":"96a690e5319c94d94923988025307e543f16fd970aec24524cf9808dc62b093359287251503f4231bf52cd1a16a80bfa82d8f585d96855dc1932f4919a92da2618d6448fc18a234f9acb386ab4ab4a9e38ea341e7c54faceff38c162d74e7fabbca13aadb71e9c8ae6072e7bef4073cf08aa7faaa6d639f98d15bad4ed183ced":"1c8f41424acaf009996ceaa815b24ad4":"":128:"9f3c0349c5a4a740a82d6d63bf00fb17":"6100b091e52366fb422251d9b68974b6c666a62a8bb77a1ffd7c7d1ae586a6ee763b84dc11aace02a25af91d194b70b3265ec46872fded54275b7ddb26ee1f20c857328f46a694fb1dce68bcaecbd587ece5b505d658d57d50333e30b639eea1f6537b37c175f62497c6c84e3cfddae214285d2d68d90dd5cd8ce2273d25c8ca":0

AES-GCM
NIST Validation (AES-192,128,1024,0,128) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"3e0ce4fb4fe4bb2fdf97b23084ff5671b9b899624184acef":"df89974b1534f0ba262bbea5efe39d8b72820cc8a720cc99520fedbf667515c3f6d8c3e25c72c48c1cff042171df58421741aacb2a49f23167257be7d7004d56b14901b2075eaca85946e9fbf1bbf4ae98227efc62bf255a25dd0402d37c67ba553531c699dd89ff797e7a5b5b9a9aa51e73ca2dacfda0f814152aa8ed8c79f9":"a950ab0dd84115e3829ab0ad3bbb1193":"":128:"25cfde73e7a29115828dfe1617f8b53e":"847b54e176ccc83081cb966efc4b4a3bf7809ce0b4885009f620f61fafcaa78feee91a835ae6c1a942571811108b1e81b4c4ddac46aaff599c14988c9a1fb9f387ab7f1357b581568b7b34e167ac2c8c2b2b8a4df3fd7ad8947a363c1c0cb782ec54b1901e928821cf319669dd77eb37b15c67f13ad787ff74312812731ca3e6":0

AES-GCM
NIST Validation (AES-192,128,1024,0,120) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"6be3c66b20e5e66ababbfba1b38e5a716eafce23a1767b69":"de1cd978354a499415176f260021abe0a8c5bc34d166f53d20e02e413e1377ce4ef5d7f58337c62251a3b4ddea0dea23c40e5de037fd5dd8a558eb53bffa4e8ce94899afa8284afab503c1a485999a154d23777f9d8a031b7ad5c6d23d6abbe3b775c77876ad50f6bed14ac0b2b88fb19c438e4b7eb03f7d4d3fcca90dd01260":"3a2acf69bba19f5d1d1947af2cfda781":"":120:"f826d212f7c1212fb8a8bf23996826":"fd1f7b56e5664cf4c91e58f7c50f6c5e98e42ca2e4adcc00348cee6f662b382ad4022da54a47d8faeb9b76a24dfc4f493c27fc0bc421a4648fad7b14b0df95d8752013feb033b1fd971daa2c9a5df898bece6a3b8fa078dd130071df20a68cd0f394be25dcbb3e85bdfa0df4797fa6f01f5f0da7a6e86320207ddb5b3be53ae0":0

AES-GCM
 NIST Validation (AES-192,128,1024,0,120) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"d16abb9f5b38d7f5abba9dc36995ce6ce928ed822a07b7c4":"e72f29b1fc1dbfc2d93a0f3b79ea4b9806ce9b2c4d490ac5c0c3c793df9dc7df5471e834b84d18afa5a7516f9a6a813a9b65ae2f083a854730547e28a1f60fe97d8dba1d2d433e11847b9bffd8873ec634e64365530c905dd6f274e45c9795ac127a6f356f63cc6c116c5dd8c628e7e17e1fadc58f8452bf21f53c4133198118":"3cd95429c6de1d327b9eb3c45424a87c":"":120:"13521236f190f78e75c0897c5fb237":"cd8bb97c28df092b6783ef653fd26f2bdc27c442bab0a4c7bee2789f389dcd1b280c0231672721bfbbc939a0449557678ec61ba0afb2e5817e6f7d94387f84ecafbfa1216d65e7f5025f47b0d2905cff7c99adf8306a3d9850c5908be05f87cb1d36a4837dba428aac97d7fbc18e3778f8d81a319259504c87fc94bd0766ed93":0

AES-GCM
 NIST Validation (AES-192,128,1024,0,120) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"0bc344b1a4078807e5f53a6e7e1e36fa83108473ae2fb4c2":"8bd73f94c71e3765bc7d17fdc90a9ba6aff9648b46300e4048985fbbd7c60c39c3766f7c524780bfc2296dc11e1132134921760a373104edc376eab6e91e9a60a5c4a5972935df12eadae074722bdc0147c3caf6a62fd449ef37d76b65f6d210283c94ac524cf13186e444d80a70b01e4373cc0462546f1caee6b49e738a742c":"bd505fcba464e6e2c58fdf29f5695fb9":"":120:"8510fff71bb879f56ea2fe43f6ff50":"FAIL":0

AES-GCM NIST Validation (AES-192,128,1024,0,112) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"c8097398fc21f93eea6a95aa93a3231096817b65520bc549":"80b0abbaebbd537a0810ed75cd172d29d50f5982e4d01f8664ddb2dfda8f57fa0ed87e64a779a1d7f5e568b6acfdc739572a7176752307b430fb1fa1c3c2c346477cebe7d01b16745ca6c8929a7f446c03ad9a9e8a5a935de78ca6c701e8c1c5e6d2550c42949cf5342fb5ef4c6ab9bb02ace8388b16edf72a1237e5d1d0e820":"776248381941e16908f52d19207881f5":"":112:"7fc4388b2f8eab0f0c2d6a08527e":"FAIL":0

AES-GCM
 NIST Validation (AES-192,128,1024,0,112) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"76d4bb5694faaf344db83bc6d6c47d56bb6ab52700826f2d":"9e31fda6a171f0d4a5f2af2c4f827b1312d9dda5d78fa329b8f1b6373b9b29be358601e5bb0d0c615aef4b9e441c811219f1f2ff2d0ab23e0cd829a88b5b615ee72e5e3ea604fa26cc6438ec4c30e90f7348e9116adf8e8efb7498320d2da16679fa546b1aa9afc7720b074c4e48e06862d41428c9e71a4772c2e195a6f36978":"603977845d82faccb401817ecce6e2fe":"":112:"c955a3bc316841be07e406d289c8":"FAIL":0

AES-GCM NIST Validation (AES-192,128,1024,0,112) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"a3e5020695587984074d78d9c98b8e1a5719e5f88372740e":"c0bfe3b2dc4dad17ec5a7662d86847fb67e582cc0baf469bc9baa7a075d48a8b97521a1072c2798bfbdae5ca3752eda1cb96fe5cf24af989eb77a2948aae3d8b70d83d93f84c49347f788480f34051621c358c03cf8159a70fc72cb8bc02876234ffe76b181da8b22b8796c87b0904da1af46de519c20d8d1b1dc7cc24e39ba5":"4cd56de54e5140a587be7dfd02d3a39e":"":112:"1a29527a41330259f918d99d7509":"FAIL":0

AES-GCM

NIST Validation (AES-192,128,1024,0,104) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"afe986ead799727063958e2ce13ca846f76c51605439f839":"7c1b354a5bb214bd95147e32d81e658705089c38035d0ea423eb1a5c82f97443c6903d2cf1ba7a007eec7c8ff98b8f82b073d9636a79bd47c7f2f639a8eb4e92076f9ed615766f43ac3a4f1687301ed7d507766605e0e332880ae740ab72e861a2cb6dce1df1ff8be1873d25845ee7c665e712c5bbe029a1788634bce122836c":"f85a95ed10b69623162ab68d1098de94":"":104:"3cf1cdb4a4fdc48da78a8b4e81":"a7f252ad7983e7083260598051bffd83f40f4d4a8b580cc2388d720a0979dde71549ddcb86b0a62c4964fca591d0982f3a203f2f8884ff4991f17e20f759ea7125ba2bb4d993722f23938994eb2709c850f33ed9889e5a3966f9d7b76add46aedf230e8f417425f9db79ccd46b5660361de7c5d87f71a9d82c491c0c3daaf56c":0

AES-GCM NIST Validation (AES-192,128,1024,0,104) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"2cfaa215841826a977ae6adfdd993346210c49dd04d5d493":"e8eb3b6edd0ca4201b49a6a83036445aba1a1db040f3e74511363bce769760a9914e05a067f555ca15a57c6e02e66fbe4e04dd8c8db8d6d14ebc01cc7d84a20ff0aacb69bb3679d6b7d9d2e07deda7c2d4fe4c584fe1166e78d21dc56b9cdad93709c03b9145b887f87b4f605f24f989d5e0534fc71a58e8a8619ee99f69e5f5":"537a4ee307af3072e745570aaaadce34":"":104:"df01cffbd3978850e07328e6b8":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,1024,0,104) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"128ddc83d2170c403a517615056dceec0d19d6fd7632e738":"cfe9f7797ee37bfc4f564419bf2268c964479efa7435970874154432930f3b2736438da4dc9c76200009651340e23044bc9d200a32acfd4df2e1b98b0bae3e9ff9d6e8181d926d2d03f89768edc35b963d341931ac57d2739b270ce254f042b64ceac4b75223b233602c9a4bdc925967b051440c28805d816abe76fc9d593f5a":"5124b410c43d875eca6ce298c45994a7":"":104:"56ad9c1653f11a41fd649cccd8":"cf91f087fd7faf362caacf4a68cff51ec57b3075563e4ad0955df20b366e92bd75c3762cf4a6f0eb859872667a5c55aa5d94f5ac9479b1b9c9345b50f82379d551506a2ab02b0441b14b28b78a12b38500d703a8c19888fe612d4710eec7cd18c16d6a4b55d3c69760e2bed99efc8b551dbe2ac9b9b64715f87180b8e14d1795":0

AES-GCM
NIST Validation (AES-192,128,1024,0,96) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"98581c28983c4da321ce0c419cc0d476d539e77da513c894":"bdef5b65b5111b29e781a6b71a0160179c52b5bccb1ac5c0377b26cf3f61432f3ccd67633a836357c24b5099db0510a7f8110f59e8227cacd11f17ea1798b5d4d68902ca6c6eccd319fef14545edd135078b38d43b61c9af269fc72f7a209ba7897e4c6dbd21bb71d7e93d2d2426ffa1557cae28e74059d3baf06ba419a47b39":"ff10234524433b871202c2cca6acb194":"":96:"984943355a7aef15c4fb8033":"808e28bfd441cb8890416a757d252c986daa8d607ac9cadd2f4fd29eddbcf3b859ba298e14a4ccefe2c2752b123f87b98d6708fde48faca4bc7dd818a7ea76cfa4357932e59cb6be0e9283bdfb49454b86b9fd04aa8cdef503c65d13fcff42e9cd8f142f8c06cf7daa6d8ef8b9c9d69c39e8afd980048fecf731fd674b2a814b":0

AES-GCM NIST Validation (AES-192,128,1024,0,96) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"167b8b6df8014c8f3de912b77f5a0c113580aa42d785298f":"4f787de12ba907a589edf74c8e7a6cdaaabebddd465a86e170e1efc289240298b516fddc43c7fd9bb1c51720a4455db4dd630b59aebaa82bd578eb3cb19f8b23ee6897c1fefaef820430efa6eb7d6ff04de4d8b079605fb520b0d33e96c28f0cd71983c4ce76c0ea62fd7209d21ec7b416881d545824a73d1f9f8d3323fdb90c":"49da91e926091a448d57d521cc90f3c

0":"":96:"99198f55f9fa763651bba58e":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,1024,0,96) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"71f5f8505fba62f08fa0557dd5407fc83a852c6007ccecc8"
:"3e19ec02365e450e946123a3362f9859352eb52902a6bcb8a782285dfac9d2b282f56302b60d6e9f53fddd16bbf0497
6cf4eb84ef3b6583e9dc2f805276a7b7340dec7abde4916fb94b0ed9c9af6d4917b27e44d25f3952d0444cd32a4a574e1
65a23fa8c93229ceb48345171a4f20d610b5be7d9e40dcf7209128f029fed6bf":"b5efb9feae3de41b5ce9aa75583b8d21
":"":96:"9604d031fa43dcd0853e641c":"FAIL":0

AES-GCM NIST Validation (AES-192,128,1024,0,64) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"4cdb38f8185a4186fc983e58a776a6454b92ecf0bffefe98"
:"1ca72c50a093076e9a9dfa09888b9c89eb36a942072fc536a81713f05a2669b39fdb2871b82ca47dcaf18393ca81dcb4
99aafcc4ed57ea79f8d4f9bd63540610215b2c65481b294638cec41264a7fdca4230df5fe1e7e3d8d26dcd0c435fec8e9b
f778f9e6f13482157a9722761601e08425f6160d3bb626ae39ee1117b0353c":"aef257dd44d14d0bc75f9311ef24e85a"
:"":64:"d951becb0d55f9fb":"2eaa7e922dbd8963e2078aae216636276f3f7cb5d7f35fa759e91bddb6e247a93c388241b
a1d0d37040c0b9e447c67d35b4991c1acce97914f3bc22ee50171bc5922299983ee70af79303265bc1ae1e7334202460
618b4a8891d1a7eaaac5cac1e4dce024ce662d14849993f89e771fb873644b552120fd346250df39aaaa403":0

AES-GCM
NIST Validation (AES-192,128,1024,0,64) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"ee8d3aced3aa3cb2166aa66c4a252c12dc0978830d0bc75
b":"ee69b2421d43a9f383d99f9802ba4d6cf1c537b42041c86cce681049bb475e5098d4181f1902b0a49c202bf34ef70e
a7b787fa685ab8f824fcc27282146d8158925bfef47ccba89aa81c0565eacb087b46b8706c9f886b7edf863701003051d
6fb57e45e61d33412591ec818d016eec7dee4254636615a43dacb4f1e6ec35702":"c15c9c0b0b70c7321df044bfde2b1
5fb":"":64:"c5c9851a6bf686d0":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,1024,0,64) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"4a8538d609444e3197ab740cd33b66db1cf53600096b94e
0":"8c2b8fb775d1b21c41a3dcf48ad6d68ab05be3879f9b94b305a6ce4d799e3a992c1c3a65a3e4eab563edb57424927
c90c76e49386e29dd5e7de2800fcc0eefbc8b4f977f71be3754c006ee93dc09b1cfa59c424b6b3987aeb56feefc21004c6
3e8284b6845e395bc8843cca0917267fb4a8f2db1f7daafe7a9da95083a44de70":"0bd64d222532dae8ab63dc299355bf
2a":"":64:"3477cad1fd4098b2":"FAIL":0

AES-GCM NIST Validation (AES-192,128,1024,0,32) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"447f0f065771b6129952e52206a64fe0844658ed685e39c
d":"fea5d227869e527882c63a68a6623f4a699df82b3dc715c7260a5554336df8376744c05ae89ec27d40da02d9f1c5e9
e29405579fd4132143cb21cdbe3edfaaab62128ecc28018725c8dd309d2376223d2e2edfea9765699b2630ff5d9fe9bec
416c0ca6418b938d195d31a08e4034c49d79e3a249edd65f985230b33c444dd02":"37e3a300542d9caf3975c6429cb8
a2e8":"":32:"06bfca29":"e1bdd1c212b159b87e41a5f64dcba6b27aa0f5c8871fabfb588df0e06bd7730ec1beb0e3388f
96c992a573ff69b34870f83c53fb65b420c1c6f92e2aa6f03917e8203d77c7f5ee08baf9fab12f9d38fc0ffb83807ba781c
3dd7b62edca2121f68ef230b42b8adbd4cea072209d02713789ed559b83739a54cfde69e68bdc4128":0

AES-GCM
NIST Validation (AES-192,128,1024,0,32) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"f465e95f6fc19fe6968b98319b547104d0c01c17105f8fc0"
:"2426f108368a00d2a49670a3b64b4f0569c6da9660163e7b209ec3f8d058ee11f7818a8c5030c5f4ce6e1e5a93faa3e5
ae3d0bd5d712fbc891cfeb20845707edcf5e29719a5246a3b024fb12d37bd1b81df3812fd50b1dfb3e948ce546dd165cc
77f903c07fe32bc7da7fbc25036679017317ce94cd8a00c1bce7379774f1714":"6cba4efc8d4840aa044a92d03d6b4d69
":"":32:"92750ac9":"2e59b104c1a6f6d651000396adbfa009bf4cf8cbf714da8e4d3b4a62bd7f522d614decf090c7552a
4b9e8d7ee457ba642d5100c0c81c14cbba8c8ff49b12827f6ebd41504ccb6dfc97cdf8532d1f7f7e603c609efa72d2ae0d
ce036ec4ab36849a0c06f8737d9710075a1daaed3867ca0a7e22111c0e7afae91f553b6fd66c6e":0

AES-GCM
NIST Validation (AES-192,128,1024,0,32) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"f08e3e9f7b3a20ccdc4d98b56f2b567399a28a6b3908deab
":"a986e816f1eafb532c716a555cca1839a1b0523410134ea0426ab309520b339fc1fdeb40478ae76823cee4e03b8d345
0e6be92d5ff17b2f78400f0176e6d6a3930bd076a7a3c87c3397dcc0520c6b7b4ff9059ea21e71c91912a74aac2ca70eec
422b507cc5c60860bb8baca01eec2a3003970ba84011efe576804b2820e306c":"4f4636d1b283bfa72c82809eb4f1251
9":"":32:"16c80a62":"FAIL":0

AES-GCM NIST Validation (AES-192,128,1024,1024,128) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"87b5372571fb244648053c99405999130f87a7c17805229
7":"ae078d1554fc6a14447a28c3dd753e790f7ef9b53e35c3e0fe63a7b1b326bc56034847f8a31c2d6358049aae990bfe
7575b439db370aa515e225e0ec730488c700a7b0a96a7b8e4e8e4c6afec20decd16fe3c0f3f8d7a6cf7a8711d170829d1
4c706cceb00e133b8c65c8e08cd984b884662eddd2258ce629abf6b9dd28688c9":"a1cc81b87bd36affe3af50546e361c
9e":"684ce23f59632308d7db14f7f6eddaf4d83271fb0c27401b09518a775b36252540f14305f0dae13ff6c0dc565c9e5
70759e070c8ac73dfb97abd3285689a7cdcfc941f6271be3b418740b42ba4a114421065a785be3dfa944c86af56da8209
779e8736e62529c418b507c6d8ae002cbc0431747722afd64521734f99273de455":128:"98177b3428e64bc98631375
905c0100f":"8be7df33a86b1162464af738de582a357d0ce8e213bba1b7913c0d13ad759d62c3bf4366f5130b3af2b25
5b7ad530b4977627f9e76b07e360c079d0f763dabbd22e976b98cd5495c6182f95bc963aad4b719446f49d3a448d11ca
c5bfcba4b675b8e4d88a389e2580e8f383f95bf85c72e698680d2a2bc993c9ee1ce0d1f1ac3":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,128) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"a2d069b826455d5e79e65db4f1d2b6a29ae9f401bc62391
7":"acd6225dc5b9109d56ea565ab38dd4db432a7ec08f0db04f1c6b691c96d2eaaa6be62da7cc7fd75f931716c7f39705
ea7cf828f1a5a325955e9b2c77e7fb2d562be6a89b3351b1b3d1355b43b73ed425049430314c16bf0836ed580e9390a3
b8e2a652fddbfa939ca4c3c99765b09db7f30bf2ef88e1aa030e68958722cb0da3":"6d40a0c7813bc0410ff73f19bb5d8
9c9":"9960376b1898618d98c327c1761959d045488cc6198238bbe72662f276d47b41e8aebc06dbce63da5adcb302a6
1ade140c72b9cf9f6dfad6ecedd7401c9509fae349d3c7debe35117776227ba167f2b75921d7321d79f4ebca13d20af163
8a1567043365f179f4162795fe4fd80b5d832e4ca70e7bf9830bc272b82182f70d2e":128:"010195091d4e1684029e58
439039d91e":"FAIL":0

AES-GCM

NIST Validation (AES-192,128,1024,1024,128) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"f3252351fe8e7c628c418c1a49709bf1f8e20add82539948":"7e8d2816d280c91d232bad43b6610e2d0532a9f670f221a3a975fb16472c2e83b168115e87a487bcd14b37f075e1faa59c42515c353cdefc728ac617b7d273fa96778e3fb5f7a1132f8e2add4a57015b15d1984338b7862356243d1c5aa628406f4a507498eda12d2f652c55e8e58113ed828783b82505790654f036b610f89a":"eacd2b1c3cf01bf4ea7582d8ee2675d5":"141cb39a2fb8e735e0c97207f1b618a4b98f6b9bf8c44a1c8e9ea575a7759cc2a02301274553e7744408b2c577b4c8c2a00e18f8717fd8a6d2f46a44eeb05d685fbef7edeb4229e7ea9b8e419ffcb504d33583b3ae421c84caeca9f9789047dd7b1810318d3765307233567bc40e003401c9f4e1b07a2a7162889e1a092aedc1":128:"63a310b4f43b421a863fb00fafd7eac4":"699c146927ae29025e5b20088b20af27bc75449e4725ee6b7d5dc60b44ba8a06f7d265330c16060fbd6def244630d056c82676be2dc85d891c63d005804085c93ce88f3f57c2d2c0371c31027d0a4a0031e3f473cb373db63d4ff8f65be9ebe74045de813a4e6c688110d000f6b12406881c08085c9348e1f0315038907e33f7":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,120) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"e462957f2c500bf2d6bfa9af97938fdd8930e360ea4175e7":"82a7a6dd82a5ea3d9a8e9541d854978487eda298b483df02b45c76b8b38bac98ffd969dd160a2765595b19d4ea3e64351ce95764a903f595dd673d13facf5a5594e01be1d60a0c6d28b866a1f93a63a74fecb6d73ac6fb26b20c008b93db53e9dc1d3e3902359fd47734fe22a5c6958f97e9001cc4e8b6484d9542dbbdfcfcdc":"b380584a3f4e0e59add4753c282f2cf7":"682b0af6592eef173e559407e7f56574c069251b92092570cbb7f5a2f05e88bed0af48dcda45b2930b1ee7d5da78dc43ec3598a38593df7c548058eda3c9275c1304489aff95f33a6cd79e724e8d12ca0ae92b20273eb3736efcd50dc49e803ad631dcbf64376a45a687eb4e417aef08a3f5f8230d3f0b266ea732c21ed2eed7":120:"28a43253d8b37795433140641e9ffd":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,120) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"4a62ddd87f41c6df756e8da0985dcd8c91e73ba395b3d79b":"37a83ee6dbdece212446739ea353cb957b9aa409c88bee042bbc3a6e5199aeb28f2b4b00ff433c0c68d6db5a197566019db8a4c7a792e2839a19a302ee02bee046adce04c1fbbd5b0c457d7cbe277992ce2c153d132269e2d1f12b084cf3026a202b4664bc9d11832e9b99c7cc5035dcfde5991dd41aeb4fbf8bec5126a9f524":"1d1843e2118772d76a0244a2c33c60bd":"028b92727b75b14cb8dfeb7a86a7fec50cd5de46aa4a34645754918b8606819d4bf8a2e7531a05ae5505492ca6cbc8c0e6d6ab2dea23bff1fdf581bb780b4a3312aa39639383fd10bcf92489801954733f16b021c2e84809345216f8f28a99773341e40c4a64305a2098eaa39f26a93bd556c97f02090e1a6c181a4e13e17d3a":120:"ab738073228bdf1e8fd4430b5c7d79":"e702f1bb9a1f395c74fca0ce9cdf29e7332c14acaca45200cd432a5767be38929ef8de43d0e1a5e7300c1eb669ac1ab997b31cb1403af8451e77e63505920af0f8c3abf5a9450ea47371039ba1cf2d65a14fa5f013b7ce1d175859404dcf6461a36e8bc260e7abf739d8951ddf1a3754e2d65e0aa31320a5ffca822023bc0906":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,120) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"fc46976d38a581a7042a94ea4b5bfe3587ddc65d1162d71e":"4b9e858fc8f01903e426112192d4ae4686b1ae4d683b75afb2b8c63590275943d0d6d6a23b6d35796a2f101203acba107474ca6f4ff6dd87d6b77785ad1d160ef2755d84092dc70c86db5e639b689943b15efa646aff44b3f51f5d3f4cf6c8f7fc5adfe7bf2d72f75b93b8ee94ef3fa69ea0fc0bb77b3983901fdcd30bcd36f5":"b5e92563dd0339df00b7ffa2239d21bc":"7b6f6e104acbcd7188161477d8e425ff99add22df4d22de7f28d0a0075ca4ef848f68d07ed22d3165c08e40890ce04d1bd05b1a6ccb2fec8193d5f7dffc93d97a0c036b3748f708b011b68247a0249b9e1a60b652164e5c2fd7210377de804ac0

10c8aa08a11f40af97e8370a59f936cd14c22ea7a236d904145adc04a241fc0":120:"d4356cb417953b01f7b1110c8aa3eb":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,112) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"403e49feadd4db763652ed5c4b1e12680cfe0abc30f4696d":"221c61d769febce3913bfead9a201a805f11005ddcac185cbae00ce749de9c4362889b1b0d9546e91598e0ddedb88b673a90acca65d7e71a85636be052f361839a646dc8b834c02f3e2261d370e6bac9636b7536225b5ea77881200c8a3450d21bfd1e11afb3a470e178ecfe944a25a7cd0254e04a42b67723aac8afffd56fee":"1a60258a56e15f92814b4d372255a80d":"a4ffa9e3c612103224c86515dad4343cbca7a7daf277f5828670834f4d9af67b9a935c71b2130dfbc929c4409bffb7974ffa87523b58890770439c33342880b33319c626bf776c1c0aeb9c2a348a7681572f4ff711d94c192f3450e8b1275f9d02c742a2c9f1da316e9918bf787f22699172986cb9b10fc56d5f6b8392ff92b8":112:"62646fc8bfe38b3ba6d62f9011e3":"5c76c90dea7d659804ad873960906259fbdda3614277ec575d9eec730e747a2e7b9df6716b4c38d3451e319eeecee74d1f4918266fc9239de87080f1ad437b47c6904ed2d5514161ad25e3e237655e00e53fe18d452576580e89b2f1f0f6aa7e40a337fd8c48d690fe013a67264a80e9b5dfd009a9152d559aa02a68f401a09b":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,112) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"c3471259512d1f03ce44c1ddac186e9a56c1434a6ac567c6":"dd5b98b3b3cf03fb92be579068a885afd984630692eb5f155fa6b49f2b1690b803d34b90e8de3cc39c2e61650ffffb51e7ef36d35ad17dc4d91f336363b0734996b162b509c9954cab3dd959bde7e437e9100d84c44104c61e29dbe12492a0272ce6eea2906d390de7808d337e8c650b3301af04a9ed52ab9ea208f3c7439d6c":"50164c63d466148ab371376d5c2b6b72":"11d1f523888bea1fbc680d34bc9b66957d651efa59e788db3d3f6f50e72184b9d14e9ff9bc05fb687520cf423d681812e007025eedf0e78e7e8191e6b62404e8eb400cf837d762a31aa248553367263d6de091fcf7abedc3e69fc118b7efb0594c89b96c387b7c28ed9a7b75db60b6b5133949b891ff81eca5790a265f12a58c":112:"6c5f38232e8a43871ab72a3419ad":"50438ee712720abf2089331e4c058b30c30c3d17834c507c0010ac3f974a256d01b14a45e9ce5193c5cede41330cf31e1a07a1f5e3ceca515cc971bfda0fbe0b823450efc30563e8ed941b0350f146ec75cd31a2c7e1e469c2dd860c0fd5b286219018d4fbacda164a40d2980aa3a27aa95f8b8e2cd8e2f5f20d79a22c3ff028":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,112) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"ec326a1e0fe6a99421398df4fc7d8fea67b67e5f5fcd50ad":"6d5016c434a0f4b4a5d9e0b6b8e2d848a94f132f055d2d847e54601a4c9cfc5966a654d696f8a3529a48a90b491ea0d31c08eae8ef364f71f8ec7ae7f7e39bb9c331137b2578362ff165628099944ba8deb0d99ac660d5ed2215b9a7626ff1fa6173cd8dd676c988d16c9cf750a0d793f584c3c8f5fd5d167bc278f4d77a629c":"c94aa4baa840a044dbd5942787a0c951":"f8401c578f20d9c250ea86eb945184e007a0190462c7abddf238ce1ceddcc230756aa222386d8ba66ebbba13de008ced140896ac55bc47c231cc81370ca9feadc225e017d59890e6291cc4cca27db3078c0cd6cbb51afb62210226a76837c5454728cb5ce3afe7352e7fe75421f94986e6b7b26321bbca15c75ac7c13dc15f50":112:"3269922affb9d767f5abe041cc8e":"FAIL":0

AES-GCM NIST Validation (AES-192,128,1024,1024,104) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"a7ef81652f604e88a72416924c53979dc73cadd3575eda1c":"9ecd19a8eba9fba843486e1bbfb8d9053c5e04b24e30174d4aa89d8307439d653f8630edddafd51719c744bcb4bce3e444847567bd2cdde2995870d0634cc0ba2bde4b6bc2bc583062fb83874a1c25b50aeb945bd109a151772c077438c4d

1caaeb5b0c56390ac23c6d117f3a00fd616306fc2ffc4c1e76f934b30fbbc52eec2":"0cc9ae54c9a85f3e9325c5f3658ab3b2":"d0195b744351aa25a57a99df9573dfa3cebe9850139149b64f7e4af37756a430dda8af98e4ed480e913aa82821c01c1f75b187e105a8f39621757d522c083a8d81d7d8bfe6cf15c439d0692b6affd655a11bcd2457046fae996a1075c66029867b88cd23c503ae04037dd41f27bafd5000d1f516002f9fcc0f2500e8c1b27de0":104:"22c2efeddfd5d9cb528861c4eb":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,104) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"605271a41e263c92dc14fe9df5203e79d58cc2d1289dc361":"2bda3448a283ecba31e0299c0a9e44628cb2b41fa7b1a41107e107cabc381083bdbe048f2804568fdd5fe016f4d607f694042a459ba03a2deda4cccc8cbe4612d8ed0d4575e48bc9f59843369dbe2af6d048e65ff4250e1eef61d7b1b378fe2f3305b133ddc7e37d95ca6de89a971730fc80da943a767ff137707a8d8a24329c":"7f128092a777fc503adc7f6b85eb2006":"aef9f984fb645e08d5f0aa07a31c114d2f8e9eca047e4a8d5471378cfc2ced1159dc093d174788e58447a854be58942ed9a3fd45f3f4a1af7351e087369a267797c525f134e79709097e733b9003b9be0c569fc70ee3462b815b6410e19954ce2efac121300c06fd9e00542a9c6a5a682fe1010c145acbbb8b82333bdb5ddfd9":104:"673afea592b2ce16bd058469f1":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,104) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"fa076f36cb678e2275561e9553ebdf397360e5a5e44791c4":"513305e86c0cb046c5d3720b25a406392766bd1fb7de2758de370ff2e68281e211922890c61f3659460f22c45a57895b424441262a3ba0606df4e2701f38281fd3436a4d0e0f8efecd231808a9ea063dfb725015a91f27cadfe7909a0ee109eac391ac807afed1767ae0515b9c1b51ae9a48b38fe7fec7fe0ddee562c945e5ae":"1ecd53d94fe287047ff184e8b9b71a26":"5ff25f7bac5f76f533f9edffdfd2b2991d7fc4cd5a0452a1031da6094cd498297fb2a05ae8db71cb3451e4ac33a01172619035a9621d2d54f812ef5343e14b9dedc93838e4cf30e223d215b4d2476ea961a17ac7295069f25b2a12d6e2efe76d91f45632c6d4e61ff19a95d5ae36af960d95050ce98b5791df0b7e322411c884":104:"079e8db9c3e6eddb0335b1cf64":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,96) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"ce9dafa0e7e53a8766fc0bc38fba807d04e14e5ed61bc234":"b585b8bf634757dac015f2f69f2ae674372a664f2115ad2d03bd3e0c335306b02d0947d3cda5991f5c0c25f12ead2c3cc2d65d575fd67091c70bc93ddb4b1e21f7b0fc6e6ae652dea93a6564ff13489f927942e64dd94bf8f821c7ffdef16df58bd8306a957821ac256da6f19c9d96e48eee87f88acb83bae05d693b70b9337b":"fd0751af49814ee98b2b0cdf730adaa6":"1cba488a0fc8a012f9a336cc7b01cbcc504178eeb08237dbedbc6c7ac68fdf3a6742751a207e43d43068abf6ef4e12a5e3c17e5a2f9398fc04ced67377cbb858fd6020fad675a880adb249e4aba94b96efa515d1cdf5c0c3071a27a3245968867ea94b2bfc2028a67be34c84c3f475944497aa8ca1ab009f8e4b11c8308c1996":96:"e5dc92f4ad4000e9b62fb637":"95f4324b0656bef19eca5570548fc6a7a9923f4e2a7e42066891bc132fd73bc1c9089755d996756de0072824e69c43f2db8ba2bf6f90d3c4eafc0721ceaccce1af896f9fb15fb19c4746979b6d945f593fad61d550f81d12b5945ed728c02931d7f8d917285c22a3af748d75a6bf163fddd84b941d8564c1a63192c816ad6d6d":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,96) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"8a328554fed68dc4838fbc89fd162c99ec105b36651abbc9

":"75986f56972c045c850ed68aeb229f203b228fdfc36cad6b16d9bd12037c48700d20d8062a983ffeca76b8d36a67ef5
1bc8853706e83a34e4e23ff4f4a4eb943f19dbe85e454043d7906be6587a85079f9ccd27962d2905117d2dbeaf725d6ffe
87bef52b2138da153ef29b18065b3342b3f9d07837d57b8bc5f2597de06c54f":"e4f7c69a1d026eeebfc45e77bd7b3538
":"e349dcedb0bfcc771c820f0d510b80cef32ae3326484e25aa183015941e7844bc46f617d5e61fd64fa71759e90fcb72
ae220bcd507f0fb389b689dd3fa29b3b937eded85f26ada9e0f3f5109f82fef47c7eba7313049750ad17969e7550c0d409
3ed18ee27843d082bcee8bf3fc7833d569b7723998595a5a1d871089fd238da":96:"8e8320912fff628f47e92430":"a1e
d65cfc7e1aeccd0531bce1dc749c7aa84451ec0f29856f12f22c4105888c7d62e2e2fc8ad7a62748610b16e57490f061ad
063c88800037d7244ee59e109d44520528047339033 6d7b6089f3a78218447b1b2398c4d0b3aac8b57a35891ad60dc1
b69ad75e2e86248ceac7bb4cf3caade4a896e5ee8c76893ef990f6f65266":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,96) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"6e7f6feb4022312de5c804ed1d7a37580d74499107f8cc8b
":"4f5bbdf575ab8f778549f749f2265e17dc7225713e73ee6d7be163ff7071557dcc2240b0705c079008605f81396414a
c64f06b1b637876e04c3fca8d0fa576cef4dd3dc553fd6808eaf120f837f9bb1d9dbbd5cf67ed497167fc7db89d3a84151
b81aeab0e921057f121583df5ed7f976b206ece17a913f23485385f64c462a8":"6ce13485ffbc80567b02dd542344d7ef
":"c6804a2bd8c34de14fe485c8b7caa2564adaf9fcbb754bd2cc1d88ba9183f13d110c762a3c5d2afc0fbc80aedcb91e45
efe43d9320075420ee85ab22505f20e77fa4624b0387346c1bd944e9cd54055b5135c7fc92e85390ecf45a7091136b47e
3d68d9076594cfad36c36047538e652178c375a2fe59a246a79784577860189":96:"974bd0c4a8cac1563a0e0ce0":"F
AIL":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,64) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"46d6e982feff0e7d04a84384c56739b69626dde500e4b7fb
":"a5160fb2d397b55a7eba02df33a042404188f02f4492d46f4edc03fc67723d64f5f7fed3a60728438703c60454a30f47
3ac918ffc8f98be5c5e9779ee984415e415ce3c71f9acc3f808d215be58535d3144cebe7982b9b527edbe41446161094d
6fc74dec2e0a1c644bbc2cf5779a22bd4117a7edb11d13e35e95feeb418d3f0":"71a6d1e022a6bdff6460c674fb0cf048"
:"67a8455c7d3fbfdba3c5ec5f40e0be935fbb9417e805771832ffad06ba38a61b8377997af1f586dc0fa1e3da0b39facd5
20db1f0ec2bdf1904a3a897f0b507c901fab30a85de51effa9f7d4703ceeb2ca72abe0bd146ba0bd3ffdee11628310db7d
65ea1343b018084ea2414995f86fefb45ba91a9dc2236d92078b4305671b5":64:"84f1efd34ff84e83":"FAIL":0

AES-GCM NIST Validation (AES-192,128,1024,1024,64) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"991dcaa2e8fdad2b4e6e462a3c06c96067ef5e9fb133496a
":"9cd0c27f0c2011c1ab947400d28516c7f46d22a409a18fd35c1babf693b8030dfd7822d9ba03bb8fd56a00f9c7149c0
56640dde690889d2f23978eeeb28ccc26e2fc251220a3682c963f5580c654c1a6736cccb1b8ed104ec7390021d244bd9f
92abde89e39a4b83eff8211c8a6259bd6ac2af1da7dfb8cf1355238056c60381":"978913d2c822ba7cc758041d5ee4675
9":"5a94dc81af011a8af263318b60215b9752292b194b89f6fc013b0fe8e29133de631d981862f2c131ee34905bd93caf
fc3b8f91aeb0264b27a509e5c6a41ae781209f8c5895d0d35b3c5e1ae34a1a92a2b979e0e62132051394940ea4d9bfffb
8d89ba1e8331b15bdf05c41db83a57745a4a651a757cc8648acdcf850a2f25367":64:"15d456da7645abf2":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,64) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"f29cff00781f5916930f125489c87d21f6593324d1506f65
":"a3e8595747b7147d471ac4fe38014bf4a409931e3f419ff88ae249ba7a7f51bd0ede371bf153bab4b28020b7a82a8ca

30b75f1e3bcfee3c13db813cbc85138ef05874dedb14a6e5b6d06d7589a83bd5e052dc64433a8e24c1188b9470ddb253
6d13b4b7bff0c5afcfaa9aa0157c3aae3b1774df2df14f965d6dee4332edba67e":"50db7ee25a9f815c784236f908bfd7f2
":"ec1482e18692bcd6894a364c4a6abb9c3b9818bb17e5e1fc9ec0b41702c423f3a60907e94c888fad8e78f51e1f724b3
9969ba7b11d31b503504b304d5c4b4cbd42634f4ec5080a9fe51c82e121ae191270dd2c307af84c82d892d982413a50c
cce33698054f761a3fa93da9a1fca321296b378a50d458ba78e57a70da4676150":64:"a1e19ef2f0d4b9f1":"eea18261a4
de31d8619e77005ebbb3998c5dcfac2bc120ae465e29d6b4c46de7e6c044c8b148ffe4eda7629c243df8af4e7ceb512d5
751a3ee58defb0690b6f26b51086dedfde38748f6f0bbe6b495f4304373188e5d2dc93461bd51bf720149a7d3aa543623
b122b9af0123b2cdc9020136b041a49498ec4aa696c2d3c46d06":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,32) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"2087e14092dad6df8996715cb1cfca90094f030328080ffd
":"6d039513061980fb195bdf2f7c7079ca4b7e0fdd50d948cbfab5ba10b99e3aea27f08abd000c428851de82cacb0d64c
146cd9567e9d55b89819876d6a635bd68bcaf47ffa41e02d9ee97f5a2363bfe6131ae7a21ea5130ae953a64d57d6cbfd4
5260c5f1946388d445ce97d23ab7ba31a5069a4896bc940a71de32bde02bc18d":"d30504afb6f8b6ac444b4a76115d79
d1":"d95845d268c8d8f9135d310c39e30f55f83ef7ffee69e6ba1f80d08e92ed473b5ac12cc8f7a872bfc8b325e6b8e374
609c90beaf52d975f71caeef5ee4c13de08dce80d358ee1cd091faea209a24e3392adcfe01aeb2b2e1738bc75d4a9b7cd3
1df7f878141cf278d150f6faa83fb3a2fd1225542a39c900606c602f15c06a4f":32:"5412f25c":"1e81a4c10a3440d0002
ddc1bfa42ebb08e504fcc8f0497915c51b6f5f75fee3f0cd3e9c5a81ff6528e0fecd68a36192114f17fa1a4cfe21918dac46
e3ba1383c2678c7a6889a980024ee2a21bcf737f7723b5735e1ebe78996f7c7eace2802ebb8284216867d73b53a370a5
7d5b587d070a96db34b5b4f5afe7f39830498c112":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,32) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"3fc76d627c775de2f789279dc7b67979a9f1cc23c8dcabc9
":"92a60d38fc687b92d44635aafee416a142d11a025680e5aa42e9ba5aa010462991ad3dd7328ca4a693673410f9bba3
7f05a551b949ab0d43fc61ef3b8996dd3fc1b325e66eec6cc61ea667500f82a83e699756a139d14be6ca9747ed38cd9b1
d9da032ece311331bdcd698666ddc970b8be2b746ec55fe60e65d7ae47c6f853c":"8f6fd53eb97e12dcd4d40f2843e253
65":"e56995df73e52606a11de9df6c7bfb0ef93b86bf6766e319aea59372060294b0e1b13c6288c2310a4bef725a2dddb
174f3e1228649861757903c4497a0eec9c141454fc75f101439a2150e368857c4f0f6e5161c42c77f632bf1c229a52595
cbf16e9018de9a8f6a1e6b8b18bd244f93f001eb2eb315405d223c0d27ece9d4d9":32:"613ba486":"FAIL":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,32) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"b10979797fb8f418a126120d45106e1779b4538751a19bf
6":"e3dc64e3c02731fe6e6ec0e899183018da347bf8bd476aa7746d7a7729d83a95f64bb732ba987468d0cede154e281
69f7bafa36559200795037ee38279e0e4ca40f9cfa85aa0c8035df9649345c8fdffd1c31528b485dfe443c1923180cc8fae
5196d16f822be4ad07e3f1234e1d218e7c8fb37a0e4480dc6717c9c09ff5c45f":"ca362e615024a1fe11286668646cc1d
e":"237d95d86a5ad46035870f576a1757eded636c7234d5ed0f8039f6f59f1333cc31cb893170d1baa98bd4e79576de9
20120ead0fdecfb343edbc2fcc556540a91607388a05d43bdb8b55f1327552feed3b620614dfcccb2b342083896cbc81d
c9670b761add998913ca813163708a45974e6d7b56dfd0511a72eb879f239d6a6d":32:"28d730ea":"dafde27aa8b3076
bfa16ab1d89207d339c4997f8a756cc3eb62c0b023976de808ab640ba4467f2b2ea83d238861229c73387594cd437703
86512ea595a70888b4c38863472279e06b923e7cf32438199b3e054ac4bc21baa8df39ddaa207ebb17fa4cad6e83ea58c
3a92ec74e6e01b0a8979af145dd31d5df29750bb91b42d45":0

AES-GCM
Bad IV (AES-192,128,0,0,32) #0
depends_on:MBEDTLS_AES_C
gcm_bad_parameters:MBEDTLS_CIPHER_ID_AES:MBEDTLS_GCM_DECRYPT:"b10979797fb8f418a126120d45106e1779b4538751a19bf6":"":"":"":32:MBEDTLS_ERR_GCM_BAD_INPUT

AES-GCM Selftest
depends_on:MBEDTLS_AES_C
gcm_selftest:
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDEwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDIwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQWHpv1i6lf
wvNPOP5ka6S0n55EvzoaYK6pbTXP6yMOW/4XZSPKx5Zoq4FMe0cKzGIIFL1rzj1V
2czYB+qvLhyio4GJMIGGMB0GA1UdDgQWBBT5RCgQ0AlZTQbfFB2+6+w0XRvydTBX
BgNVHSMEUDBOgBSh3uHkX5nj86yFEFwjscSWM40P+qEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAI7unGW/gr9tOc3i+dF5N815srgh+FrX
oj9Et74EcSpTAiBubv+vOH0DE0gmYI11HeAIgutWqqMIC72dZlwTF/Vi3g==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB3jCCAYWgAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDAwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQznn9zHHwL
GO8VR4W9V7vMlxCdoojzEOiX5Y6JtPtFOz866ueHY6zoN0/mJ6DnqnSXilJIUUeW
6eGfqmka7nxko4GRMIGOMB0GA1UdDgQWBBSh3uHkX5nj86yFEFwjscSWM40P+jBf
BgNVHSMEWDBWgBQlFYvU5WboI4fcdPoiQs8/fPHZraEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggkA/KCWhcqToHAw
DAYDVR0TBAUwAwEB/zAKBggqhkjOPQQDAgNHADBEAiBasbuinP+pJTU4oDCVD8zQ
1rJBDSOKIEyWu84/D6Hj6wIgVMPUoO01bPhzllAa/gW8Xk/daey09SBgN3AT9pWU
TDA=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIBpTCCAUugAwIBAgIJAPygloXKk6BwMAoGCCqGSM49BAMCMC8xCzAJBgNVBAYT
AlVLMREwDwYDVQQKDAhtYmVkIFRMUzENMAsGA1UEAwwEQ0EwMDAeFw0xNzA2MjIx
MTUwMzJaFw0yNzA2MjMxMTUwMzJaMC8xCzAJBgNVBAYTAlVLMREwDwYDVQQKDAht
YmVkIFRMUzENMAsGA1UEAwwEQ0EwMDBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IA
BFW41/qAwAPpy+Txdc7PKmzZsq9CPiujKU4vpF1ekXnGx2HP420QobwBVVWhkzRm
LwdboH2j65dcCKjQ7mv/dxKjUDBOMB0GA1UdDgQWBBQlFYvU5WboI4fcdPoiQs8/
fPHZrTAfBgNVHSMEGDAWgBQlFYvU5WboI4fcdPoiQs8/fPHZrTAMBgNVHRMEBTAD
AQH/MAoGCCqGSM49BAMCA0gAMEUCIQC7iRcVzwMyfVK5imirJ7MqJQ04euH4CLOt
IZ+SNfaERAIgSU0MWFDosVEIpg8YMqIHeF7Mg4ZyH6+fGazJgVLttUY=
-----END
CERTIFICATE-----

```
option(USE_STATIC_MBEDTLS_LIBRARY "Build mbed TLS static library." ON)
option(USE_SHARED_MBEDTLS_LIBRARY "Build mbed TLS shared library." OFF)
option(LINK_WITH_PTHREAD "Explicitly link mbed TLS library to pthread." OFF)

set(src_crypto
  aes.c
  aesni.c
  arc4.c
  asn1parse.c
  asn1write.c
  base64.c
  bignum.c
  blowfish.c
  camellia.c
  ccm.c
  cipher.c
  cipher_wrap.c
  cmac.c
  ctr_drbg.c
  des.c
  dhm.c
  ecdh.c
  ecdsa.c
  ecjpake.c
  ecp.c
  ecp_curves.c
  entropy.c
  entropy_poll.c
  error.c
  gcm.c
  havege.c
  hmac_drbg.c
  md.c
  md2.c
  md4.c
  md5.c
  md_wrap.c
  memory_buffer_alloc.c
  oid.c
  padlock.c
  pem.c
  pk.c
  pk_wrap.c
  pkcs12.c
  pkcs5.c
  pkparse.c
  pkwrite.c
  platform.c
```

```
  ripemd160.c
  rsa.c
  sha1.c
  sha256.c
  sha512.c
  threading.c
  timing.c
  version.c
  version_features.c
  xtea.c
)

set(src_x509
  certs.c
  pkcs11.c
  x509.c
  x509_create.c
   x509_crl.c
  x509_crt.c
  x509_csr.c
  x509write_crt.c
  x509write_csr.c
)

set(src_tls
  debug.c
  net_sockets.c
  ssl_cache.c
  ssl_ciphersuites.c
  ssl_cli.c
  ssl_cookie.c
  ssl_srv.c
  ssl_ticket.c
  ssl_tls.c
)

if(CMAKE_COMPILER_IS_GNUCC)
  set(CMAKE_C_FLAGS "${CMAKE_C_FLAGS} -Wmissing-declarations -Wmissing-prototypes")
endif(CMAKE_COMPILER_IS_GNUCC)

if(CMAKE_COMPILER_IS_CLANG)
  set(CMAKE_C_FLAGS "${CMAKE_C_FLAGS} -Wmissing-declarations -Wmissing-prototypes -
Wdocumentation -Wno-documentation-deprecated-sync -Wunreachable-code")
endif(CMAKE_COMPILER_IS_CLANG)

if(WIN32)
  set(libs ${libs} ws2_32)
endif(WIN32)
```

```
if(USE_PKCS11_HELPER_LIBRARY)
  set(libs ${libs} pkcs11-helper)
endif(USE_PKCS11_HELPER_LIBRARY)

if(ENABLE_ZLIB_SUPPORT)
  set(libs ${libs} ${ZLIB_LIBRARIES})
endif(ENABLE_ZLIB_SUPPORT)

if(LINK_WITH_PTHREAD)
  set(libs ${libs} pthread)
endif()

if (NOT USE_STATIC_MBEDTLS_LIBRARY AND NOT USE_SHARED_MBEDTLS_LIBRARY)
  message(FATAL_ERROR
 "Need to choose static or shared mbedtls build!")
endif(NOT USE_STATIC_MBEDTLS_LIBRARY AND NOT USE_SHARED_MBEDTLS_LIBRARY)

if(USE_STATIC_MBEDTLS_LIBRARY AND USE_SHARED_MBEDTLS_LIBRARY)
  set(mbedtls_static_target "mbedtls_static")
  set(mbedx509_static_target "mbedx509_static")
  set(mbedcrypto_static_target "mbedcrypto_static")
elseif(USE_STATIC_MBEDTLS_LIBRARY)
  set(mbedtls_static_target "mbedtls")
  set(mbedx509_static_target "mbedx509")
  set(mbedcrypto_static_target "mbedcrypto")
endif()

if(USE_STATIC_MBEDTLS_LIBRARY)
  add_library(${mbedcrypto_static_target} STATIC ${src_crypto})
  set_target_properties(${mbedcrypto_static_target} PROPERTIES OUTPUT_NAME mbedcrypto)
  target_link_libraries(${mbedcrypto_static_target} ${libs})

  add_library(${mbedx509_static_target} STATIC ${src_x509})
  set_target_properties(${mbedx509_static_target} PROPERTIES OUTPUT_NAME mbedx509)
  target_link_libraries(${mbedx509_static_target} ${libs} ${mbedcrypto_static_target})

   add_library(${mbedtls_static_target} STATIC ${src_tls})
  set_target_properties(${mbedtls_static_target} PROPERTIES OUTPUT_NAME mbedtls)
  target_link_libraries(${mbedtls_static_target} ${libs} ${mbedx509_static_target})

  install(TARGETS ${mbedtls_static_target} ${mbedx509_static_target} ${mbedcrypto_static_target}
        DESTINATION ${LIB_INSTALL_DIR}
        PERMISSIONS OWNER_READ OWNER_WRITE OWNER_EXECUTE GROUP_READ
GROUP_EXECUTE WORLD_READ WORLD_EXECUTE)
endif(USE_STATIC_MBEDTLS_LIBRARY)

if(USE_SHARED_MBEDTLS_LIBRARY)
```

```
  add_library(mbedcrypto SHARED ${src_crypto})
  set_target_properties(mbedcrypto PROPERTIES VERSION 2.6.0 SOVERSION 0)
  target_link_libraries(mbedcrypto ${libs})

  add_library(mbedx509 SHARED ${src_x509})
  set_target_properties(mbedx509 PROPERTIES VERSION 2.6.0 SOVERSION 0)
  target_link_libraries(mbedx509 ${libs} mbedcrypto)

  add_library(mbedtls SHARED ${src_tls})
  set_target_properties(mbedtls PROPERTIES VERSION
 2.6.0 SOVERSION 10)
  target_link_libraries(mbedtls ${libs} mbedx509)

  install(TARGETS mbedtls mbedx509 mbedcrypto
        DESTINATION ${LIB_INSTALL_DIR}
        PERMISSIONS OWNER_READ OWNER_WRITE OWNER_EXECUTE GROUP_READ
GROUP_EXECUTE WORLD_READ WORLD_EXECUTE)
endif(USE_SHARED_MBEDTLS_LIBRARY)

add_custom_target(lib DEPENDS mbedcrypto mbedx509 mbedtls)
if(USE_STATIC_MBEDTLS_LIBRARY AND USE_SHARED_MBEDTLS_LIBRARY)
  add_dependencies(lib mbedcrypto_static mbedx509_static mbedtls_static)
endif()
-----BEGIN EC PARAMETERS-----
BggqhkjOPQMBBw==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIJETLWqIZtnejCGzESDgMnknxqEx5evMGZfzBVPKMwKKoAoGCCqGSM49
AwEHoUQDQgAErHPyZDXGH2zIKTn6y+ZCjhsTiWhkukkCHjTt91HgaU6HtW1NmnDe
udsY73BqNHyRLcYNn3Dx0YU5xjAQ9btTdg==
-----END EC PRIVATE KEY-----
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
```

```
    <Configuration>Release</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid>{46CF2D25-6A36-4189-B59C-E4815388E554}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>mbedTLS</RootNamespace>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>StaticLibrary</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>StaticLibrary</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
  <ConfigurationType>StaticLibrary</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'"
 Label="Configuration">
  <ConfigurationType>StaticLibrary</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')"
 Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
```

```
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
   <LinkIncremental>true</LinkIncremental>
    <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <LinkIncremental>false</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
   <LinkIncremental>false</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <ClCompile>
     <PrecompiledHeader>
     </PrecompiledHeader>
     <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_WINDOWS;_USRDLL;MBEDTLS_EXPORTS;%(PreprocessorDefi
nitions)</PreprocessorDefinitions>
     <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
     <CompileAs>CompileAsC</CompileAs>
    </ClCompile>
   <Link>
     <SubSystem>Windows</SubSystem>
     <GenerateDebugInformation>true</GenerateDebugInformation>
   </Link>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
   <ClCompile>
     <PrecompiledHeader>
     </PrecompiledHeader>
     <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_WINDOWS;_USRDLL;MBEDTLS_EXPORTS;%(PreprocessorDefi
nitions)</PreprocessorDefinitions>
     <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
```

```
    <CompileAs>CompileAsC</CompileAs>
  </ClCompile>
  <Link>
    <SubSystem>Windows</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
  </Link>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
     </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_WINDOWS;_USRDLL;MBEDTLS_EXPORTS;%(PreprocessorDef
initions)</PreprocessorDefinitions>
    <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Windows</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
  </Link>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_WINDOWS;_USRDLL;MBEDTLS_EXPORTS;%(PreprocessorDef
initions)</PreprocessorDefinitions>
    <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Windows</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
  </Link>
 </ItemDefinitionGroup>
 <ItemGroup>
  <ClInclude Include="..\..\include\mbedtls\aes.h" />
  <ClInclude Include="..\..\include\mbedtls\aesni.h" />
```

```
  <ClInclude Include="..\..\include\mbedtls\arc4.h" />
  <ClInclude Include="..\..\include\mbedtls\asn1.h" />
  <ClInclude Include="..\..\include\mbedtls\asn1write.h" />
  <ClInclude Include="..\..\include\mbedtls\base64.h" />
  <ClInclude Include="..\..\include\mbedtls\bignum.h" />
  <ClInclude Include="..\..\include\mbedtls\blowfish.h"
/>
  <ClInclude Include="..\..\include\mbedtls\bn_mul.h" />
  <ClInclude Include="..\..\include\mbedtls\camellia.h" />
  <ClInclude Include="..\..\include\mbedtls\ccm.h" />
  <ClInclude Include="..\..\include\mbedtls\certs.h" />
  <ClInclude Include="..\..\include\mbedtls\check_config.h" />
  <ClInclude Include="..\..\include\mbedtls\cipher.h" />
  <ClInclude Include="..\..\include\mbedtls\cipher_internal.h" />
  <ClInclude Include="..\..\include\mbedtls\cmac.h" />
  <ClInclude Include="..\..\include\mbedtls\compat-1.3.h" />
  <ClInclude Include="..\..\include\mbedtls\config.h" />
  <ClInclude Include="..\..\include\mbedtls\ctr_drbg.h" />
  <ClInclude Include="..\..\include\mbedtls\debug.h" />
  <ClInclude Include="..\..\include\mbedtls\des.h" />
  <ClInclude Include="..\..\include\mbedtls\dhm.h" />
  <ClInclude Include="..\..\include\mbedtls\ecdh.h" />
  <ClInclude Include="..\..\include\mbedtls\ecdsa.h" />
  <ClInclude
Include="..\..\include\mbedtls\ecjpake.h" />
  <ClInclude Include="..\..\include\mbedtls\ecp.h" />
  <ClInclude Include="..\..\include\mbedtls\ecp_internal.h" />
  <ClInclude Include="..\..\include\mbedtls\entropy.h" />
  <ClInclude Include="..\..\include\mbedtls\entropy_poll.h" />
  <ClInclude Include="..\..\include\mbedtls\error.h" />
  <ClInclude Include="..\..\include\mbedtls\gcm.h" />
  <ClInclude Include="..\..\include\mbedtls\havege.h" />
  <ClInclude Include="..\..\include\mbedtls\hmac_drbg.h" />
  <ClInclude Include="..\..\include\mbedtls\md.h" />
  <ClInclude Include="..\..\include\mbedtls\md2.h" />
  <ClInclude Include="..\..\include\mbedtls\md4.h" />
  <ClInclude Include="..\..\include\mbedtls\md5.h" />
  <ClInclude Include="..\..\include\mbedtls\md_internal.h" />
  <ClInclude Include="..\..\include\mbedtls\memory_buffer_alloc.h" />
  <ClInclude Include="..\..\include\mbedtls\net.h" />
  <ClInclude Include="..\..\include\mbedtls\net_sockets.h"
/>
  <ClInclude Include="..\..\include\mbedtls\oid.h" />
  <ClInclude Include="..\..\include\mbedtls\padlock.h" />
  <ClInclude Include="..\..\include\mbedtls\pem.h" />
  <ClInclude Include="..\..\include\mbedtls\pk.h" />
  <ClInclude Include="..\..\include\mbedtls\pk_internal.h" />
  <ClInclude Include="..\..\include\mbedtls\pkcs11.h" />
```

```
  <ClInclude Include="..\..\include\mbedtls\pkcs12.h" />
  <ClInclude Include="..\..\include\mbedtls\pkcs5.h" />
  <ClInclude Include="..\..\include\mbedtls\platform.h" />
  <ClInclude Include="..\..\include\mbedtls\platform_time.h" />
  <ClInclude Include="..\..\include\mbedtls\ripemd160.h" />
  <ClInclude Include="..\..\include\mbedtls\rsa.h" />
  <ClInclude Include="..\..\include\mbedtls\sha1.h" />
  <ClInclude Include="..\..\include\mbedtls\sha256.h" />
  <ClInclude Include="..\..\include\mbedtls\sha512.h" />
  <ClInclude Include="..\..\include\mbedtls\ssl.h" />
  <ClInclude Include="..\..\include\mbedtls\ssl_cache.h"
/>
  <ClInclude Include="..\..\include\mbedtls\ssl_ciphersuites.h" />
  <ClInclude Include="..\..\include\mbedtls\ssl_cookie.h" />
  <ClInclude Include="..\..\include\mbedtls\ssl_internal.h" />
  <ClInclude Include="..\..\include\mbedtls\ssl_ticket.h" />
  <ClInclude Include="..\..\include\mbedtls\threading.h" />
  <ClInclude Include="..\..\include\mbedtls\timing.h" />
  <ClInclude Include="..\..\include\mbedtls\version.h" />
  <ClInclude Include="..\..\include\mbedtls\x509.h" />
  <ClInclude Include="..\..\include\mbedtls\x509_crl.h" />
  <ClInclude Include="..\..\include\mbedtls\x509_crt.h" />
  <ClInclude Include="..\..\include\mbedtls\x509_csr.h" />
  <ClInclude Include="..\..\include\mbedtls\xtea.h" />
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\library\aes.c" />
  <ClCompile Include="..\..\library\aesni.c" />
  <ClCompile Include="..\..\library\arc4.c" />
  <ClCompile Include="..\..\library\asn1parse.c"
/>
  <ClCompile Include="..\..\library\asn1write.c" />
  <ClCompile Include="..\..\library\base64.c" />
  <ClCompile Include="..\..\library\bignum.c" />
  <ClCompile Include="..\..\library\blowfish.c" />
  <ClCompile Include="..\..\library\camellia.c" />
  <ClCompile Include="..\..\library\ccm.c" />
  <ClCompile Include="..\..\library\certs.c" />
  <ClCompile Include="..\..\library\cipher.c" />
  <ClCompile Include="..\..\library\cipher_wrap.c" />
  <ClCompile Include="..\..\library\cmac.c" />
  <ClCompile Include="..\..\library\ctr_drbg.c" />
  <ClCompile Include="..\..\library\debug.c" />
  <ClCompile Include="..\..\library\des.c" />
  <ClCompile Include="..\..\library\dhm.c" />
  <ClCompile Include="..\..\library\ecdh.c" />
  <ClCompile Include="..\..\library\ecdsa.c" />
  <ClCompile Include="..\..\library\ecjpake.c" />
```

```
  <ClCompile Include="..\..\library\ecp.c" />
  <ClCompile Include="..\..\library\ecp_curves.c"
/>
  <ClCompile Include="..\..\library\entropy.c" />
  <ClCompile Include="..\..\library\entropy_poll.c" />
  <ClCompile Include="..\..\library\error.c" />
  <ClCompile Include="..\..\library\gcm.c" />
  <ClCompile Include="..\..\library\havege.c" />
  <ClCompile Include="..\..\library\hmac_drbg.c" />
  <ClCompile Include="..\..\library\md.c" />
  <ClCompile Include="..\..\library\md2.c" />
  <ClCompile Include="..\..\library\md4.c" />
  <ClCompile Include="..\..\library\md5.c" />
  <ClCompile Include="..\..\library\md_wrap.c" />
  <ClCompile Include="..\..\library\memory_buffer_alloc.c" />
  <ClCompile Include="..\..\library\net_sockets.c" />
  <ClCompile Include="..\..\library\oid.c" />
  <ClCompile Include="..\..\library\padlock.c" />
  <ClCompile Include="..\..\library\pem.c" />
  <ClCompile Include="..\..\library\pk.c" />
  <ClCompile Include="..\..\library\pk_wrap.c" />
  <ClCompile Include="..\..\library\pkcs11.c"
/>
  <ClCompile Include="..\..\library\pkcs12.c" />
  <ClCompile Include="..\..\library\pkcs5.c" />
  <ClCompile Include="..\..\library\pkparse.c" />
  <ClCompile Include="..\..\library\pkwrite.c" />
  <ClCompile Include="..\..\library\platform.c" />
  <ClCompile Include="..\..\library\ripemd160.c" />
  <ClCompile Include="..\..\library\rsa.c" />
  <ClCompile Include="..\..\library\sha1.c" />
  <ClCompile Include="..\..\library\sha256.c" />
  <ClCompile Include="..\..\library\sha512.c" />
  <ClCompile Include="..\..\library\ssl_cache.c" />
  <ClCompile Include="..\..\library\ssl_ciphersuites.c" />
  <ClCompile Include="..\..\library\ssl_cli.c" />
  <ClCompile Include="..\..\library\ssl_cookie.c" />
  <ClCompile Include="..\..\library\ssl_srv.c" />
  <ClCompile Include="..\..\library\ssl_ticket.c" />
  <ClCompile Include="..\..\library\ssl_tls.c" />
  <ClCompile Include="..\..\library\threading.c" />
  <ClCompile Include="..\..\library\timing.c"
/>
  <ClCompile Include="..\..\library\version.c" />
  <ClCompile Include="..\..\library\version_features.c" />
  <ClCompile Include="..\..\library\x509.c" />
  <ClCompile Include="..\..\library\x509_create.c" />
  <ClCompile Include="..\..\library\x509_crl.c" />
```

```
  <ClCompile Include="..\..\library\x509_crt.c" />
  <ClCompile Include="..\..\library\x509_csr.c" />
  <ClCompile Include="..\..\library\x509write_crt.c" />
  <ClCompile Include="..\..\library\x509write_csr.c" />
  <ClCompile Include="..\..\library\xtea.c" />
 </ItemGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
   <Configuration>Release</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\ssl\ssl_server2.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">

   <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid>{A4DA7463-1047-BDF5-E1B3-5632CB573F41}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>ssl_server2</RootNamespace>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
```

```
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
/>
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <LinkIncremental>true</LinkIncremental>
```

```
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
     <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
 <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
```

```
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
   </Link>
   <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
   </ProjectReference>
  </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
   <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
   </Link>
  </ItemDefinitionGroup>
   <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
   <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
   <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
   </Link>
  </ItemDefinitionGroup>
```

```
 <Import
 Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
DES Encrypt and decrypt 0 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:0:-1

DES Encrypt and decrypt 1 byte
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:1:-1

DES Encrypt and decrypt 2 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:2:-1

DES Encrypt and decrypt 7 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:7:-1

DES Encrypt and decrypt 8 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:8:-1

DES Encrypt and decrypt 9 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:9:-1

DES Encrypt and decrypt
 15 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:15:-1

DES Encrypt and decrypt 16 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:16:-1

DES Encrypt and decrypt 17 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:17:-1

DES Encrypt and decrypt 31 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:31:-1

DES Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
```

enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:32:-1

DES Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:33:-1

DES Encrypt and decrypt
47 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:47:-1

DES Encrypt and decrypt 48 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:48:-1

DES Encrypt and decrypt 49 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:49:-1

DES Encrypt and decrypt 0 bytes with one and zeros padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:0:MBEDTLS_PADDING_ONE_AND_ZEROS

DES Encrypt and decrypt 1 byte with one and zeros padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:1:MBEDTLS_PADDING_ONE_AND_ZEROS

DES Encrypt and decrypt 2 bytes with one and zeros padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:2:MBEDTLS_PADDING_ONE_AND_ZEROS

DES
Encrypt and decrypt 7 bytes with one and zeros padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:7:MBEDTLS_PADDING_ONE_AND_ZEROS

DES Encrypt and decrypt 8 bytes with one and zeros padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:8:MBEDTLS_PADDING_ONE_AND_ZEROS

DES Encrypt and decrypt 9 bytes with one and zeros padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:9:MBEDTLS_PADDING_ONE_AND_ZEROS

DES Encrypt and decrypt 15 bytes with one and zeros padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:15:MBEDTLS_PADDING_ONE_AND_ZEROS

DES
Encrypt and decrypt 16 bytes with one and zeros padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:16:MBEDTLS_PADDING_ONE_AND_ZEROS

DES Encrypt and decrypt 17 bytes with one and zeros padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:17:MBEDTLS_PADDING_ONE_AND_ZEROS

DES Encrypt and decrypt 31 bytes with one and zeros padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:31:MBEDTLS_PADDING_ONE_AND_ZEROS

DES Encrypt and decrypt 32 bytes with one and zeros padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:32:MBEDTLS_PADDING_ONE_AND_ZEROS

DES Encrypt and decrypt 32 bytes with one and zeros padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:33:MBEDTLS_PADDING_ONE_AND_ZEROS

DES
Encrypt and decrypt 47 bytes with one and zeros padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:47:MBEDTLS_PADDING_ONE_AND_ZEROS

DES Encrypt and decrypt 48 bytes with one and zeros padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:48:MBEDTLS_PADDING_ONE_AND_ZEROS

DES Encrypt and decrypt 49 bytes with one and zeros padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:49:MBEDTLS_PADDING_ONE_AND_ZEROS

DES Encrypt and decrypt 0 bytes with zeros and len padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:0:MBEDTLS_PADDING_ZEROS_AND_LEN

DES Encrypt and decrypt
1 byte with zeros and len padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:1:MBEDTLS_PADDING_ZEROS_AND_LEN

DES Encrypt and decrypt 2 bytes with zeros and len padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:2:MBEDTLS_PADDING_ZEROS_AND_LEN

DES Encrypt and decrypt 7 bytes with zeros and len padding

depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:7:MBEDTLS_PADDING_ZEROS_AND_LEN

DES Encrypt and decrypt 8 bytes with zeros and len padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:8:MBEDTLS_PADDING_ZEROS_AND_LEN

DES Encrypt and decrypt 9 bytes with zeros and len padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:9:MBEDTLS_PADDING_ZEROS_AND_LEN

DES
Encrypt and decrypt 15 bytes with zeros and len padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:15:MBEDTLS_PADDING_ZEROS_AND_LEN

DES Encrypt and decrypt 16 bytes with zeros and len padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:16:MBEDTLS_PADDING_ZEROS_AND_LEN

DES Encrypt and decrypt 17 bytes with zeros and len padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:17:MBEDTLS_PADDING_ZEROS_AND_LEN

DES Encrypt and decrypt 31 bytes with zeros and len padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:31:MBEDTLS_PADDING_ZEROS_AND_LEN

DES Encrypt and decrypt 32 bytes with zeros and len
padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:32:MBEDTLS_PADDING_ZEROS_AND_LEN

DES Encrypt and decrypt 32 bytes with zeros and len padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:33:MBEDTLS_PADDING_ZEROS_AND_LEN

DES Encrypt and decrypt 47 bytes with zeros and len padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:47:MBEDTLS_PADDING_ZEROS_AND_LEN

DES Encrypt and decrypt 48 bytes with zeros and len padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:48:MBEDTLS_PADDING_ZEROS_AND_LEN

DES Encrypt and decrypt 49 bytes with zeros and len padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:49:MBEDTLS_PADDING_ZEROS_AND_LEN

DES
Encrypt and decrypt 0 bytes with zeros padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:0:MBEDTLS_PADDING_ZEROS

DES Encrypt and decrypt 1 byte with zeros padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:1:MBEDTLS_PADDING_ZEROS

DES Encrypt and decrypt 2 bytes with zeros padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:2:MBEDTLS_PADDING_ZEROS

DES Encrypt and decrypt 7 bytes with zeros padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:7:MBEDTLS_PADDING_ZEROS

DES Encrypt and decrypt 8 bytes with zeros padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:8:MBEDTLS_PADDING_ZEROS

DES
Encrypt and decrypt 9 bytes with zeros padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:9:MBEDTLS_PADDING_ZEROS

DES Encrypt and decrypt 15 bytes with zeros padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:15:MBEDTLS_PADDING_ZEROS

DES Encrypt and decrypt 16 bytes with zeros padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:16:MBEDTLS_PADDING_ZEROS

DES Encrypt and decrypt 17 bytes with zeros padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:17:MBEDTLS_PADDING_ZEROS

DES Encrypt and decrypt 31 bytes with zeros padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:31:MBEDTLS_PADDING_ZEROS

DES
Encrypt and decrypt 32 bytes with zeros padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:32:MBEDTLS_PADDING_ZEROS

DES Encrypt and decrypt 32 bytes with zeros padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:33:MBEDTLS_PADDING_ZEROS

DES Encrypt and decrypt 47 bytes with zeros padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:47:MBEDTLS_PADDING_ZEROS

DES Encrypt and decrypt 48 bytes with zeros padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:48:MBEDTLS_PADDING_ZEROS

DES Encrypt and decrypt 49 bytes with zeros padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:49:MBEDTLS_PADDING_ZEROS

DES
Encrypt and decrypt 0 bytes with no padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:0:MBEDTLS_PADDING_NONE

DES Encrypt and decrypt 8 bytes with no padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:8:MBEDTLS_PADDING_NONE

DES Encrypt and decrypt 16 bytes with no padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:16:MBEDTLS_PADDING_NONE

DES Encrypt and decrypt 32 bytes with no padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:32:MBEDTLS_PADDING_NONE

DES Encrypt and decrypt 48 bytes with no padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_CBC:"DES-CBC":64:48:MBEDTLS_PADDING_NONE

DES
Try encrypting 1 bytes with no padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_DES_CBC:MBEDTLS_PADDING_NONE:64:1:MBEDTLS_ERR_CIPHER_FUL
L_BLOCK_EXPECTED

DES Try encrypting 2 bytes with no padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_DES_CBC:MBEDTLS_PADDING_NONE:64:2:MBEDTLS_ERR_CIPHER_FUL
L_BLOCK_EXPECTED

DES Try encrypting 7 bytes with no padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_DES_CBC:MBEDTLS_PADDING_NONE:64:7:MBEDTLS_ERR_CIPHER_FUL
L_BLOCK_EXPECTED

DES Try encrypting 9 bytes with no padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_DES_CBC:MBEDTLS_PADDING_NONE:64:9:MBEDTLS_ERR_CIPHER_FUL
L_BLOCK_EXPECTED

DES Try encrypting 15 bytes with
no padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_DES_CBC:MBEDTLS_PADDING_NONE:64:15:MBEDTLS_ERR_CIPHER_FUL
L_BLOCK_EXPECTED

DES Try encrypting 17 bytes with no padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_DES_CBC:MBEDTLS_PADDING_NONE:64:17:MBEDTLS_ERR_CIPHER_FUL
L_BLOCK_EXPECTED

DES Try encrypting 31 bytes with no padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_DES_CBC:MBEDTLS_PADDING_NONE:64:31:MBEDTLS_ERR_CIPHER_FUL
L_BLOCK_EXPECTED

DES Try encrypting 33 bytes with no padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_DES_CBC:MBEDTLS_PADDING_NONE:64:33:MBEDTLS_ERR_CIPHER_FUL
L_BLOCK_EXPECTED

DES Try encrypting 47 bytes with no padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_DES_CBC:MBEDTLS_PADDING_NONE:64:47:MBEDTLS_ERR_CIPHER_FUL
L_BLOCK_EXPECTED

DES
Try encrypting 49 bytes with no padding
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_DES_CBC:MBEDTLS_PADDING_NONE:64:49:MBEDTLS_ERR_CIPHER_FUL
L_BLOCK_EXPECTED

DES Encrypt and decrypt 0 bytes in multiple parts
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_CBC:64:0:0:

DES Encrypt and decrypt 1 bytes in multiple parts 1
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7

enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_CBC:64:1:0:

DES Encrypt and decrypt 1 bytes in multiple parts 2
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_CBC:64:0:1:

DES Encrypt and decrypt 16 bytes in multiple parts 1
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_CBC:64:16:0:

DES
Encrypt and decrypt 16 bytes in multiple parts 2
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_CBC:64:0:16:

DES Encrypt and decrypt 16 bytes in multiple parts 3
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_CBC:64:1:15:

DES Encrypt and decrypt 16 bytes in multiple parts 4
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_CBC:64:15:1:

DES Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_CBC:64:15:7:

DES Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_CBC:64:16:6:

DES Encrypt and decrypt 22 bytes in multiple
parts 1
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_CBC:64:17:6:

DES Encrypt and decrypt 32 bytes in multiple parts 1
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_CBC:64:16:16:

DES Encrypt and decrypt 0 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_EDE_CBC:"DES-EDE-CBC":128:0:-1

DES3 Encrypt and decrypt 1 byte
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_EDE_CBC:"DES-EDE-CBC":128:1:-1

DES3 Encrypt and decrypt 2 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_EDE_CBC:"DES-EDE-CBC":128:2:-1

DES3 Encrypt and decrypt 7 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_EDE_CBC:"DES-EDE-CBC":128:7:-1

DES3
Encrypt and decrypt 8 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_EDE_CBC:"DES-EDE-CBC":128:8:-1

DES3 Encrypt and decrypt 9 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_EDE_CBC:"DES-EDE-CBC":128:9:-1

DES3 Encrypt and decrypt 15 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_EDE_CBC:"DES-EDE-CBC":128:15:-1

DES3 Encrypt and decrypt 16 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_EDE_CBC:"DES-EDE-CBC":128:16:-1

DES3 Encrypt and decrypt 17 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_EDE_CBC:"DES-EDE-CBC":128:17:-1

DES3 Encrypt and decrypt 31 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_EDE_CBC:"DES-EDE-CBC":128:31:-1

DES3
Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_EDE_CBC:"DES-EDE-CBC":128:32:-1

DES3 Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_EDE_CBC:"DES-EDE-CBC":128:33:-1

DES3 Encrypt and decrypt 47 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_EDE_CBC:"DES-EDE-CBC":128:47:-1

DES3 Encrypt and decrypt 48 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7

enc_dec_buf:MBEDTLS_CIPHER_DES_EDE_CBC:"DES-EDE-CBC":128:48:-1

DES3 Encrypt and decrypt 49 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_EDE_CBC:"DES-EDE-CBC":128:49:-1

DES3 Encrypt and decrypt 0 bytes in multiple
parts
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_EDE_CBC:128:0:0:

DES3 Encrypt and decrypt 1 bytes in multiple parts 1
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_EDE_CBC:128:1:0:

DES3 Encrypt and decrypt 1 bytes in multiple parts 2
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_EDE_CBC:128:0:1:

DES3 Encrypt and decrypt 16 bytes in multiple parts 1
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_EDE_CBC:128:16:0:

DES3 Encrypt and decrypt 16 bytes in multiple parts 2
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_EDE_CBC:128:0:16:

DES3 Encrypt and decrypt 16 bytes in multiple parts 3
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_EDE_CBC:128:1:15:

DES3
Encrypt and decrypt 16 bytes in multiple parts 4
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_EDE_CBC:128:15:1:

DES3 Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_EDE_CBC:128:15:7:

DES3 Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_EDE_CBC:128:16:6:

DES3 Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_EDE_CBC:128:17:6:

DES3 Encrypt and decrypt 32 bytes in multiple parts 1
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_EDE_CBC:128:16:16:

DES3
Encrypt and decrypt 0 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_EDE3_CBC:"DES-EDE3-CBC":192:0:-1

DES3 Encrypt and decrypt 1 byte
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_EDE3_CBC:"DES-EDE3-CBC":192:1:-1

DES3 Encrypt and decrypt 2 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_EDE3_CBC:"DES-EDE3-CBC":192:2:-1

DES3 Encrypt and decrypt 7 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_EDE3_CBC:"DES-EDE3-CBC":192:7:-1

DES3 Encrypt and decrypt 8 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_EDE3_CBC:"DES-EDE3-CBC":192:8:-1

DES3 Encrypt and decrypt 9 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_EDE3_CBC:"DES-EDE3-CBC":192:9:-1

DES3
Encrypt and decrypt 15 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_EDE3_CBC:"DES-EDE3-CBC":192:15:-1

DES3 Encrypt and decrypt 16 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_EDE3_CBC:"DES-EDE3-CBC":192:16:-1

DES3 Encrypt and decrypt 17 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_EDE3_CBC:"DES-EDE3-CBC":192:17:-1

DES3 Encrypt and decrypt 31 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_EDE3_CBC:"DES-EDE3-CBC":192:31:-1

DES3 Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7

enc_dec_buf:MBEDTLS_CIPHER_DES_EDE3_CBC:"DES-EDE3-CBC":192:32:-1

DES3
Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_EDE3_CBC:"DES-EDE3-CBC":192:33:-1

DES3 Encrypt and decrypt 47 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_EDE3_CBC:"DES-EDE3-CBC":192:47:-1

DES3 Encrypt and decrypt 48 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_EDE3_CBC:"DES-EDE3-CBC":192:48:-1

DES3 Encrypt and decrypt 49 bytes
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_DES_EDE3_CBC:"DES-EDE3-CBC":192:49:-1

DES3 Encrypt and decrypt 0 bytes in multiple parts
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_EDE3_CBC:192:0:0:

DES3 Encrypt and decrypt 1 bytes in multiple parts 1
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_EDE3_CBC:192:1:0:

DES3
Encrypt and decrypt 1 bytes in multiple parts 2
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_EDE3_CBC:192:0:1:

DES3 Encrypt and decrypt 16 bytes in multiple parts 1
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_EDE3_CBC:192:16:0:

DES3 Encrypt and decrypt 16 bytes in multiple parts 2
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_EDE3_CBC:192:0:16:

DES3 Encrypt and decrypt 16 bytes in multiple parts 3
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_EDE3_CBC:192:1:15:

DES3 Encrypt and decrypt 16 bytes in multiple parts 4
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_EDE3_CBC:192:15:1:

DES3
Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_EDE3_CBC:192:15:7:

DES3 Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_EDE3_CBC:192:16:6:

DES3 Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_EDE3_CBC:192:17:6:

DES3 Encrypt and decrypt 32 bytes in multiple parts 1
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_DES_EDE3_CBC:192:16:16:

DES ECB Encrypt test vector (OpenSSL) #1
depends_on:MBEDTLS_DES_C
test_vec_ecb:MBEDTLS_CIPHER_DES_ECB:MBEDTLS_ENCRYPT:"0000000000000000":"0000000000000000
":"8CA64DE9C1B123A7":0

DES
ECB Encrypt test vector (OpenSSL) #2
depends_on:MBEDTLS_DES_C
test_vec_ecb:MBEDTLS_CIPHER_DES_ECB:MBEDTLS_ENCRYPT:"FFFFFFFFFFFFFFFF":"FFFFFFFFFFFF
FFFF":"7359B2163E4EDC58":0

DES ECB Encrypt test vector (OpenSSL) #3
depends_on:MBEDTLS_DES_C
test_vec_ecb:MBEDTLS_CIPHER_DES_ECB:MBEDTLS_ENCRYPT:"FEDCBA9876543210":"0123456789ABC
DEF":"ED39D950FA74BCC4":0

DES ECB Decrypt test vector (OpenSSL) #1
depends_on:MBEDTLS_DES_C
test_vec_ecb:MBEDTLS_CIPHER_DES_ECB:MBEDTLS_DECRYPT:"0000000000000000":"8CA64DE9C1B12
3A7":"0000000000000000":0

DES ECB Decrypt test vector (OpenSSL) #2
depends_on:MBEDTLS_DES_C
test_vec_ecb:MBEDTLS_CIPHER_DES_ECB:MBEDTLS_DECRYPT:"FFFFFFFFFFFFFFFF":"7359B2163E4ED
C58":"FFFFFFFFFFFFFFFF":0

DES ECB Decrypt test vector (OpenSSL) #3
depends_on:MBEDTLS_DES_C
test_vec_ecb:MBEDTLS_CIPHER_DES_ECB:MBEDTLS_DECRYPT:"43297FAD38E373FE":"EA676B2CB7DB
2B7A":"762514B829BF486A":0

```
DES3-EDE ECB Encrypt test vector (OpenSSL) #1
depends_on:MBEDTLS_DES_C
test_vec_ecb:MBEDTLS_CIPHER_DES_EDE_ECB:MBEDTLS_ENCRYPT:"0000000000000000FFFFFFFFFFFF
FFFFF":"0000000000000000":"9295B59BB384736E":0

DES3-EDE
 ECB Encrypt test vector (OpenSSL) #2
depends_on:MBEDTLS_DES_C
test_vec_ecb:MBEDTLS_CIPHER_DES_EDE_ECB:MBEDTLS_ENCRYPT:"FFFFFFFFFFFFFFFF30000000000
00000":"FFFFFFFFFFFFFFFF":"199E9D6DF39AA816":0

DES3-EDE ECB Decrypt test vector (OpenSSL) #1
depends_on:MBEDTLS_DES_C
test_vec_ecb:MBEDTLS_CIPHER_DES_EDE_ECB:MBEDTLS_DECRYPT:"0000000000000000FFFFFFFFFFFF
FFFFF":"9295B59BB384736E":"0000000000000000":0

DES3-EDE ECB Decrypt test vector (OpenSSL) #2
depends_on:MBEDTLS_DES_C
test_vec_ecb:MBEDTLS_CIPHER_DES_EDE_ECB:MBEDTLS_DECRYPT:"FFFFFFFFFFFFFFFF30000000000
00000":"199E9D6DF39AA816":"FFFFFFFFFFFFFFFF":0
add_subdirectory(aes)
add_subdirectory(hash)
add_subdirectory(pkey)
add_subdirectory(random)
add_subdirectory(ssl)
add_subdirectory(test)
add_subdirectory(x509)
add_subdirectory(util)
Certificate:
  Data:
      Version: 3 (0x2)
      Serial Number: 10 (0xa)
      Signature Algorithm: sha384WithRSAEncryption
      Issuer: C=NL, O=PolarSSL, CN=PolarSSL Test CA
      Validity
         Not Before: Feb 12 14:44:07 2011 GMT
         Not After : Feb 12 14:44:07 2021 GMT
      Subject: C=NL, O=PolarSSL, CN=PolarSSL Cert SHA384
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
         RSA Public Key: (2048 bit)
            Modulus (2048 bit):
               00:b9:3c:4a:c5:c8:a3:8e:90:17:a4:9e:52:aa:71:
               75:26:61:80:e7:c7:b5:6d:8c:ff:aa:b6:41:26:b7:
               be:11:ad:5c:73:16:0c:64:11:48:04:ff:d6:e1:3b:
               05:db:89:bb:b3:97:09:d5:1c:14:dd:68:87:39:b0:
               3d:71:cb:e2:76:d0:1a:d8:18:2d:80:1b:54:f6:e5:
               44:9a:f1:cb:af:61:2e:df:49:0d:9d:09:b7:ed:b1:
```

fd:3c:fd:3c:fa:24:cf:5d:bf:7c:e4:53:e7:25:b5:
ea:44:22:e9:26:d3:ea:20:94:9e:e6:61:67:ba:2e:
07:67:0b:03:2f:a2:09:ed:f0:33:8f:0b:ce:10:ef:
67:a4:c6:08:da:c1:ed:c2:3f:d7:4a:dd:15:3d:f9:
5e:1c:81:60:46:3e:b5:b3:3d:2f:a6:de:47:1c:bc:
92:ae:eb:df:27:6b:16:56:b7:dc:ec:d1:55:57:a5:
6e:ec:75:25:f5:b7:7b:df:ab:d2:3a:5a:91:98:7d:
97:17:0b:13:0a:a7:6b:4a:8b:c1:47:30:fb:3a:f8:
41:04:d5:c1:df:b8:1d:bf:7b:01:a5:65:a2:e0:1e:
36:b7:a6:5c:cc:30:5a:f8:cd:6f:cd:f1:19:62:25:
ca:01:e3:35:7f:fa:20:f5:dc:fd:69:b2:6a:00:7d:
17:f7
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
X509v3 Subject Key Identifier:
7D:E4:9C:6B:E6:F9:71:7D:46:D2:12:3D:AD:6B:1D:FD:C2:AA:78:4C
X509v3 Authority Key Identifier:
keyid:B4:5A:E4:A5:B3:DE:D2:52:F6:B9:D5:A6:95:0F:EB:3E:BC:C7:FD:FF

Signature Algorithm: sha384WithRSAEncryption
68:e6:03:f0:ba:44:e7:cc:e1:b2:07:6c:56:c8:be:b7:ba:80:
61:c8:f9:66:57:e1:cb:60:7d:cd:8d:0f:66:b0:f2:61:45:fd:
fc:c8:93:95:bb:b4:14:00:76:c7:e1:57:a6:e2:60:31:8b:fc:
e1:0f:68:24:4c:bb:1d:c5:b6:77:ec:23:e1:5b:4f:10:6c:6a:
e0:6d:e7:34:f8:72:14:ae:16:57:25:8b:e8:b9:71:a1:d0:78:
ea:18:c1:51:c4:2e:26:6d:cb:80:8d:a5:b9:de:e7:37:c1:2b:
ec:e8:98:c6:f9:1a:bf:fe:a3:de:3d:d6:59:98:45:dc:4a:a6:
ad:0a:af:73:50:43:23:5a:9b:9a:f9:8f:ff:41:15:e5:9c:12:
9e:29:55:5c:79:9c:89:0c:c8:8a:82:86:b1:96:ae:7c:7d:4f:
0b:fd:e3:9e:8b:a5:4d:88:55:05:ad:6c:63:aa:74:0c:41:0d:
47:22:cc:1a:45:02:92:5e:d1:e0:b9:31:52:ff:f6:30:f0:87:
2c:dd:fa:fa:b9:cc:45:cb:36:33:5b:35:7f:5f:05:4f:e0:8f:
9a:e4:d2:fa:c9:d4:fc:62:99:ac:59:fb:fd:04:bc:5a:c0:47:
5e:5d:3d:df:31:8c:7f:dc:00:cb:cb:c0:f4:62:41:44:db:1d:
ba:c0:ad:8a
-----BEGIN
CERTIFICATE-----
MIIDQjCCAiqgAwIBAgIBCjANBgkqhkiG9w0BAQwFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTEwMjEyMTQ0NDA3WhcNMjEwMjEyMTQ0NDA3WjA/MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxHTAbBgNVBAMTFFBvbGFyU1NMIENlcnQgU0hBMzg0MIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuTxKxcijjpAXpJ5SqnF1JmGA
58e1bYz/qrZBJre+Ea1ccxYMZBFIBP/W4TsF24m7s5cJ1RwU3WiHObA9ccvidtAa
2BgtgBtU9uVEmvHLr2Eu30kNnQm37bH9PP08+iTPXb985FPnJbXqRCLpJtPqIJSe
5mFnui4HZwsDL6IJ7fAzjwvOEO9npMYI2sHtwj/XSt0VPfleHIFgRj61sz0vpt5H
HLySruvfJ2sWVrfc7NFVV6Vu7HUl9bd736vSOlqRmH2XFwsTCqdrSovBRzD7OvhB

BNXB37gdv3sBpWWi4B42t6ZczDBa+M1vzfEZYiXKAeM1f/og9dz9abJqAH0X9wID
AQABo00wSzAJBgNVHRMEAjAAMB0GA1UdDgQWBBR95Jxr5vlxfUbSEj2tax39wqp4
TDAfBgNVHSMEGDAWgBS0WuSls97SUva51aaVD+s+vMf9/zANBgkqhkiG9w0BAQwF
AAOCAQEAaOYD8LpE58zhsgdsVsi+t7qAYcj5Zlfhy2B9zY0PZrDyYUX9/MiTlbu0
FAB2x+FXpuJgMYv84Q9oJEy7HcW2d+wj4VtPEGxq4G3nNPhyFK4WVyWL6LlxodB4
6hjBUcQuJm3LgI2lud7nN8Er7OiYxvkav/6j3j3WWZhF3EqmrQqvc1BDI1qbmvmP
/0EV5ZwSnilVXHmciQzIioKGsZaufH1PC/3jnoulTYhVBa1sY6p0DEENRyLMGkUC
kl7R4LkxUv/2MPCHLN36+rnMRcs2M1s1f18FT+CPmuTS+snU/GKZrFn7/QS8WsBH
Xl093zGMf9wAy8vA9GJBRNsdusCtig==
-----END
CERTIFICATE-----
-----BEGIN PUBLIC KEY-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA5F2mqEsdntPAEij6HfCY
nKiLMGnm6PcfsaFYeFYO1EufOjN5ZJP90cr3CrCnN9JOAdpBbTpzA0RcIcAdWBzv
NNAtIMvSfi22WJYVjzD0Bvs2rCYH76Yc6vfx7y9zXZcanh8S/2t7B64xmxOWL4RE
+f8HWTijAWlyUFDk+DuJWpQK2o0bhE4S8mX+uUl3afNW5CiPsRky1N1v4a7/J2b7
cG+7pDWUcjnvmNCN84v+gSucXfKg/LiAnZgY7xih2ePEhkkIqn6kU0cVBQj1cZ7h
XGRaZ/MnqZ2y+KjiuFot2saNk/v0vjjW+xOx76qJV99LtN/1qvCYnO1RqMv2EM8W
hErLcgiRrihzaz3a2GaumL30CcNixrEXRyEjFaO/klqkpuZRHTtyUnkvhUkPUHuH
n45XPxZ7a2XRyrSbFyyS0amTjQwQCveSRiJFjK5TZ56CVGKF/DmuLSHeTY3vwi+W
XVdKMYQ6Zi9jwFJo/S4TRpzp+DTSH68FrFRqE1+qIVyWQjmhWxuvPhqVkG0IT7CZ
0M8lWesysyI759f5D8DhEp/KbWLDeXWCzcNSbgWGHW5JA+fCV7+8m0PqodIy5D8L
hwm2tI5dA6Qcro8X127RWVaVsN8LIzdf1THXfnZIm1fDBNUfhXapKfnFV8EvALFX
2Gy8M3kZQ3slaGegILfqRKcCAwEAAQ==
-----END PUBLIC KEY-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDIwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDMwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQRDXDNIi1p
ereudhqwa2LslXgsxnB63Hu5y5lg+1WPruIYPzD/Ho0APveVdzFLVji19+bE4+tF
PYL1SpsN1WfWo4GJMIGGMB0GA1UdDgQWBBQApzZdtBdD3dLxouQpr/aDiVttdzBX
BgNVHSMEUDBOgBT5RCgQ0AlZTQbfFB2+6+w0XRvydaEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAxggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAOnd+7bAofkHVa4KFNjv3TCegw1lrhuM
8Of8wgvrTEGoAiEAsS8iKMpSfXH4D0egg4gLamE6akde965rDtySU+ve9lg=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDEwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDIwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQWHpv1i6lf
wvNPOP5ka6S0n55EvzoaYK6pbTXP6yMOW/4XZSPKx5Zoq4FMe0cKzGIIFL1rzj1V
2czYB+qvLhyio4GJMIGGMB0GA1UdDgQWBBT5RCgQ0AlZTQbfFB2+6+w0XRvydTBX
BgNVHSMEUDBOgBSh3uHkX5nj86yFEFwjscSWM40P+qEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAI7unGW/gr9tOc3i+dF5N815srgh+FrX
oj9Et74EcSpTAiBubv+vOH0DE0gmYI11HeAIgutWqqMIC72dZlwTF/Vi3g==

-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB3jCCAYWgAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDAwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQznn9zHHwL
GO8VR4W9V7vMlxCdoojzEOiX5Y6JtPtFOz866ueHY6zoN0/mJ6DnqnSXilJIUUeW
6eGfqmka7nxko4GRMIGOMB0GA1UdDgQWBBSh3uHkX5nj86yFEFwjscSWM40P+jBf
BgNVHSMEWDBWgBQlFYvU5WboI4fcdPoiQs8/fPHZraEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggkA/KCWhcqToHAw
DAYDVR0TBAUwAwEB/zAKBggqhkjOPQQDAgNHADBEAiBasbuinP+pJTU4oDCVD8zQ
1rJBDSOKIEyWu84/D6Hj6wIgVMPUoO01bPhzllAa/gW8Xk/daey09SBgN3AT9pWU
TDA=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIBpTCCAUugAwIBAgIJAPygloXKk6BwMAoGCCqGSM49BAMCMC8xCzAJBgNVBAYT
AlVLMREwDwYDVQQKDAhtYmVkIFRMUzENMAsGA1UEAwwEQ0EwMDAeFw0xNzA2MjIx
MTUwMzJaFw0yNzA2MjMxMTUwMzJaMC8xCzAJBgNVBAYTAlVLMREwDwYDVQQKDAht
YmVkIFRMUzENMAsGA1UEAwwEQ0EwMDBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IA
BFW41/qAwAPpy+Txdc7PKmzZsq9CPiujKU4vpF1ekXnGx2HP420QobwBVVWhkzRm
LwdboH2j65dcCKjQ7mv/dxKjUDBOMB0GA1UdDgQWBBQlFYvU5WboI4fcdPoiQs8/
fPHZrTAfBgNVHSMEGDAWgBQlFYvU5WboI4fcdPoiQs8/fPHZrTAMBgNVHRMEBTAD
AQH/MAoGCCqGSM49BAMCA0gAMEUCIQC7iRcVzwMyfVK5imirJ7MqJQ04euH4CLOt
IZ+SNfaERAIgSU0MWFDosVEIpg8YMqIHeF7Mg4ZyH6+fGazJgVLttUY=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDYwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDcwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASNOj4d4MEA
7p/3miijqG4ToE4opKPAm+3BTIGrJTYT14++TSiUICl0ASXj+xeUcLMIaXTN042s
LsHxpShzQaL0o4GJMIGGMB0GA1UdDgQWBBREq5J3toJPxZ3O+ssJ5vkkU0RJEzBX
BgNVHSMEUDBOgBSjovYaC/m6Li9Tp0V9iZRs9267Q6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA1ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAKGcf+c442c/XiwubbaiQvsoZ7EoVxuM
oKmia0gPyBNkAiEA83asjJ5FDXQuLyZpczviXrbmqgCPOfYadtvkc0cxMis=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIBzTCCAXKgAwIBAgIMU6LLSxJOrYN9qJSyMAoGCCqGSM49BAMCMEcxEzARBgNV
BAMTCnNlbGZzaWduZWQxEDAOBgNVBAsTB3Rlc3RpbmcxETAPBgNVBAoTCFBvbGFy
U1NMMQswCQYDVQQGEwJOTDAiGA8yMDE0MDYxOTExMzY0M1oYDzIwMjQwNjE4MTEz
NjQzWjBHMRMwEQYDVQQDEwpzZWxmc2lnbmVkMRAwDgYDVQQLEwd0ZXN0aW5nMREw
DwYDVQQKEwhQb2xhclNTTDELMAkGA1UEBhMCTkwwWTATBgcqhkjOPQIBBggqhkjO
PQMBBwNCAAQ3zFbZdgkeWnI+x1kt/yBu7nz5BpF00K0UtfdoIllikk7lANgjEf/q
L9I0XV0WvYqIwmt3DVXNiioO+gHItO3/o0AwPjAMBgNVHRMBAf8EAjAAMA8GA1Ud
DwEB/wQFAwMHgAAwHQYDVR0OBBYEFLZtURgXjmWq8uzV8wHkbFLCNB1bMAoGCCqG

```
SM49BAMCA0kAMEYCIQCf/bzFoge0pCOIrtHrABgc1+Cl9kjlsICpduXhdHUMOwIh
AOJ+nBHfaEGyF4PRJvn/jMDeIaH1zisinVzC2v+JQOWq
-----END CERTIFICATE-----
0o0*H=*H=U0S38IoSIKs0m42Qu0pSrgvtT$,hTxX'
-----BEGIN EC PARAMETERS-----
BggqhkjOPQMBBw==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIPW9zE8cjiZ8w17jTAebb4xAmEg6heEEnEaG4lGCd38joAoGCCqGSM49
AwEHoUQDQgAEFh6b9YupX8LzTzj+ZGuktJ+eRL86GmCuqW01z+sjDlv+F2UjyseW
aKuBTHtHCsxiCBS9a849VdnM2Afqry4cog==
-----END EC PRIVATE KEY-----
set(libs
  mbedtls
)

if(USE_PKCS11_HELPER_LIBRARY)
  set(libs ${libs} pkcs11-helper)
endif(USE_PKCS11_HELPER_LIBRARY)

if(ENABLE_ZLIB_SUPPORT)
  set(libs ${libs} ${ZLIB_LIBRARIES})
endif(ENABLE_ZLIB_SUPPORT)

find_package(Perl)
if(NOT PERL_FOUND)
  message(FATAL_ERROR "Cannot build test suites without Perl")
endif()

function(add_test_suite suite_name)
  if(ARGV1)
    set(data_name ${ARGV1})
  else()
    set(data_name ${suite_name})
  endif()

  add_custom_command(
    OUTPUT test_suite_${data_name}.c
    COMMAND ${PERL_EXECUTABLE} ${CMAKE_CURRENT_SOURCE_DIR}/scripts/generate_code.pl
${CMAKE_CURRENT_SOURCE_DIR}/suites test_suite_${suite_name} test_suite_${data_name}
    DEPENDS ${CMAKE_CURRENT_SOURCE_DIR}/scripts/generate_code.pl mbedtls suites/helpers.function
suites/main_test.function suites/test_suite_${suite_name}.function suites/test_suite_${data_name}.data
  )

  include_directories(${CMAKE_CURRENT_SOURCE_DIR})
  add_executable(test_suite_${data_name}
 test_suite_${data_name}.c)
  target_link_libraries(test_suite_${data_name} ${libs})
```

```
  add_test(${data_name}-suite test_suite_${data_name})
endfunction(add_test_suite)

if(CMAKE_COMPILER_IS_GNUCC OR CMAKE_COMPILER_IS_CLANG)
  set(CMAKE_C_FLAGS "${CMAKE_C_FLAGS} -Wno-unused-function")
endif(CMAKE_COMPILER_IS_GNUCC OR CMAKE_COMPILER_IS_CLANG)

if(MSVC)
  # If a warning level has been defined, suppress all warnings for test code
  set(CMAKE_C_FLAGS "${CMAKE_C_FLAGS} /W0")
  set(CMAKE_C_FLAGS "${CMAKE_C_FLAGS} /WX-")
endif(MSVC)

add_test_suite(aes aes.ecb)
add_test_suite(aes aes.cbc)
add_test_suite(aes aes.cfb)
add_test_suite(aes aes.rest)
add_test_suite(arc4)
add_test_suite(asn1write)
add_test_suite(base64)
add_test_suite(blowfish)
add_test_suite(camellia)
add_test_suite(ccm)
add_test_suite(cipher cipher.aes)
add_test_suite(cipher cipher.arc4)
add_test_suite(cipher cipher.blowfish)
add_test_suite(cipher cipher.camellia)
add_test_suite(cipher cipher.ccm)
add_test_suite(cipher
 cipher.des)
add_test_suite(cipher cipher.gcm)
add_test_suite(cipher cipher.null)
add_test_suite(cipher cipher.padding)
add_test_suite(cmac)
add_test_suite(ctr_drbg)
add_test_suite(debug)
add_test_suite(des)
add_test_suite(dhm)
add_test_suite(ecdh)
add_test_suite(ecdsa)
add_test_suite(ecjpake)
add_test_suite(ecp)
add_test_suite(entropy)
add_test_suite(error)
add_test_suite(gcm gcm.aes128_en)
add_test_suite(gcm gcm.aes192_en)
add_test_suite(gcm gcm.aes256_en)
add_test_suite(gcm gcm.aes128_de)
```

```
add_test_suite(gcm gcm.aes192_de)
add_test_suite(gcm gcm.aes256_de)
add_test_suite(gcm gcm.camellia)
add_test_suite(hmac_drbg hmac_drbg.misc)
add_test_suite(hmac_drbg hmac_drbg.no_reseed)
add_test_suite(hmac_drbg hmac_drbg.nopr)
add_test_suite(hmac_drbg hmac_drbg.pr)
add_test_suite(md)
add_test_suite(mdx)
add_test_suite(memory_buffer_alloc)
add_test_suite(mpi)
add_test_suite(pem)
add_test_suite(pkcs1_v15)
add_test_suite(pkcs1_v21)
add_test_suite(pkcs5)
add_test_suite(pk)
add_test_suite(pkparse)
add_test_suite(pkwrite)
add_test_suite(shax)
add_test_suite(ssl)
add_test_suite(timing)
add_test_suite(rsa)
add_test_suite(version)
add_test_suite(xtea)
add_test_suite(x509parse)
add_test_suite(x509write)

#
 Make data_files available in an out-of-source build
if (NOT ${CMAKE_CURRENT_BINARY_DIR} STREQUAL ${CMAKE_CURRENT_SOURCE_DIR})
  # Get OS dependent path to use in `execute_process`
  file(TO_NATIVE_PATH "${CMAKE_CURRENT_BINARY_DIR}/data_files" link)
  file(TO_NATIVE_PATH "${CMAKE_CURRENT_SOURCE_DIR}/data_files" target)

  if (NOT EXISTS ${link})
    if (CMAKE_HOST_UNIX)
      set(command ln -s ${target} ${link})
    else()
      set(command cmd.exe /c mklink /j ${link} ${target})
    endif()

    execute_process(COMMAND ${command}
                    RESULT_VARIABLE result
                    ERROR_VARIABLE output)

    if (NOT ${result} EQUAL 0)
      message(FATAL_ERROR "Could not create symbolic link for: ${target} -->
```

```
 ${output}")
      endif()
   endif()
endif()
-----BEGIN CERTIFICATE-----
MIIDwjCCAaqgAwIBAgIBEDANBgkqhkiG9w0BAQsFADBIMQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxJjAkBgNVBAMTHVBvbGFyU1NMIFRlc3QgSW50ZXJt
ZWRpYXRlIENBMB4XDTEzMDkyNDE2MTIyNFoXDTIzMDkyMjE2MTIyNFowNDELMAkG
A1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NMMRIwEAYDVQQDEwlsb2NhbGhvc3Qw
WTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQcbffp2qXqoZyychmoCRxzrd4Vu96m
47NPBehtEC46aTeXgDnBdf++znABrAtfXBRNQz8ARIeYBmskr22rlKjyo4GVMIGS
MAkGA1UdEwQCMAAwHQYDVR0OBBYEFNIK06V3H85VsFxGoo5zbL+hYCa7MGYGA1Ud
IwRfMF2AFDh32Gt3nCh3gotO2BupHveUFrcOoUKkQDA+MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0GC
AQ4wDQYJKoZIhvcNAQELBQADggIBADRoQ5fHKw+vkl0D3aqLX1XrZidb+25AWbhr
FYXdaskN219PrXBL3cV8x5tK6qsPKSyyw1lue80OmhXs/w7PJkOHHUSWRnmTv7lr
8Us3Zr/yOF/VVqzdGs7DlOTpyzEBdugI9uar/aCqHDoltN8wOduOoQB9aojYpROj
+gjlEO0mgt/87XpjYOig1o0jv44QYDQZQzpj1zeIn6WMe6xk9YDwCLMjRIpg++c7
QyxvcEJTn80wX1SaEBM2gau97G7bORLMwBVkMT4oSY+iKYgpPpawOnMJbqUP73Dm
yfJExDdrW/BbWZ/vKIcSqSZIbkHdkNjUDVHczyVwQxZxzvLFw/B1k9s7jYFsi5eK
TNAdXFa4et1H2sd+uhu24GxsjmJioDrftixcgzPVBjDCjH8QWkBEX292WJ58on0e
deWLpZUnzPdE1B4rsiPw1Vg28mGgr2O1xgBQr/fx6A+8ItNTzAXbZfEcult9ypwM
0b6YDNe5IvdKk8iwz3mof0VNy47K6xoCaE/fxxWkjoXK8x2wfswGeP2QgUzQE93b
OtjdHpsG1c7gIVFQmKATyAPUz4vqmezgNRleXU0oL0PYtoCmKQ51UjNMUfmO9xCj
VJaNa2iTQ5Dgic+CW4TYAgj5/9g9X3WfwnDNxrZ0UxxawGElczHXqbrNleTtPaKp
a8Si6UK5
-----END
 CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEATCCA4egAwIBAgIBDjAKBggqhkjOPQQDAjA+MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EwHhcN
MTMwOTI0MTU1NTE0WhcNMjMwOTIyMTU1NTE0WjBIMQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxJjAkBgNVBAMTHVBvbGFyU1NMIFRlc3QgSW50ZXJtZWRp
YXRlIENBMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAo1Oc8nr6fMTq
vowV+CpC55i5BZGFGc50Eb4RLBSRTH1e7JepdFjAVbBtyQRJSiY1ja0tgLQDDKZR
wfEI+b4azse460InPHv7C1TN0upXlxuj6m9B1IlP+sBaM7WBC6dVfPO+jVMIxgkF
CaBCLhhdK1Fjf8HjkT/PkctWnho8NTwivc9+nqRZjXe/eIcqm5HwjDDhu+gz+o0g
Vz9MfZNi1JyCrOyNZcy+cr2QeNnNVGnFq8xTxtu6dLunhpmLFj2mm0Vjwa7Ypj5q
AjpqTMtDvqbRuToyoyzajhMNcCAf7gwzIupJJFVdjdtgYAcQwzikwF5HoITJzzJ2
qgxF7CmvGZNb7G99mLdLdhtclH3wAQKHYwEGJo7XKyNEuHPQgB+e0cg1SD1HqlAM
uCfGGTWQ6me7Bjan3t0NzoTdDq6IpKTesbaY+/9e2xn8DCrhBKLXQMZFDZqUoLYA
kGPOEGgvlPnIIXAawouxCaNYEh5Uw871YMSPT28rLdFr49dwYOtDg9foA8hDIW2P
d6KXbrZteesvA1nYzEOs+3AjrbT79Md2W8Bz9bqBVNlNOESSqm4kiCJFmslm/6br
Np0MSQd+o22PQ4xRtmP6UsTfU0ueiMpYc8TYYhMbfnfFyo4m707ebcflPbBEN2dg
updQ66cvfCJB0QJt9upafY0lpdV1qUkCAwEAAaOBoDCBnTAdBgNVHQ4EFgQUOHfY
a3ecKHeCi07YG6ke95QWtw4wbgYDVR0jBGcwZYAUnW0gJEkBPyvLeLUZvH4kydv7
NnyhQqRAMD4xCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UE
AxMTUG9sYXJzc2wgVGVzdCBFQyBDQYIJAMFD4n5iQ8zoMAwGA1UdEwQFMAMBAf8w
```

CgYIKoZIzj0EAwIDaAAwZQIxAPyE+u+eP7gRrSFjQicmpYg8jiFUCYEowWY2zuOG
i1HXYwmpDHfasQ3rNSuf/gHvjwIwbSSjumDk+uYNci/KMELDsD0MFHxZhhBc9Hp9
Af5cNR8KhzegznL6amRObGGKmX1F
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIICUjCCAdegAwIBAgIJAMFD4n5iQ8zoMAoGCCqGSM49BAMCMD4xCzAJBgNVBAYT
Ak5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBF
QyBDQTAeFw0xMzA5MjQxNTQ5NDhaFw0yMzA5MjIxNTQ5NDhaMD4xCzAJBgNVBAYT
Ak5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBF
QyBDQTB2MBAGByqGSM49AgEGBSuBBAAiA2IABMPaKzRBN1gvh1b+/Im6KUNLTuBu
ww5XUzM5WNRStJGVOQsj318XJGJI/BqVKc4sLYfCiFKAr9ZqqyHduNMcbli4yuiy
aY7zQa0pw7RfdadHb9UZKVVpmlM7ILRmFmAzHqOBoDCBnTAdBgNVHQ4EFgQUnW0g
JEkBPyvLeLUZvH4kydv7NnwwbgYDVR0jBGcwZYAUnW0gJEkBPyvLeLUZvH4kydv7
NnyhQqRAMD4xCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UE
AxMTUG9sYXJzc2wgVGVzdCBFQyBDQYIJAMFD4n5iQ8zoMAwGA1UdEwQFMAMBAf8w
CgYIKoZIzj0EAwIDaQAwZgIxAMO0YnNWKJUAfXgSJtJxexn4ipg+kv4znuR50v56
t4d0PCu412mUC6Nnd7izvtE2MgIxAP1nnJQjZ8BWukszFQDG48wxCCyci9qpdSMv
uCjn8pwUOkABXK8Mss90fzCfCEOtIA==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB5DCCAWmgAwIBAgIBPjAKBggqhkjOPQQDAjA+MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EwHhcN
MTQwNDEwMTcyMTU0WhcNMjQwNDA3MTcyMTU0WjA0MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxEjAQBgNVBAMTCWxvY2FsaG9zdDBZMBMGByqGSM49AgEG
CCqGSM49AwEHA0IABDfMVtl2CR5acj7HWS3/IG7ufPkGkXTQrRS192giWWKSTuUA
2CMR/+ov0jRdXRa9iojCa3cNVc2KKg76Aci07f+jYjBgMAkGA1UdEwQCMAAwHQYD
VR0OBBYEFFBhpY/UB9nXggEM5WV/jGNGpxO+MB8GA1UdIwQYMBaAFJ1tICRJAT8r
y3i1Gbx+JMnb+zZ8MBMGA1UdJQQMMAoGCCsGAQUFBwMBMAoGCCqGSM49BAMCA2kA
MGYCMQDQzjWB0xZs/8IsqJb7owYYtCiT17939Uuc/1yBF69pJRy7KV/qJlHNvlVu
qwWVTx0CMQDNW/0dlX1gU6ashrZv5Ly4sijg/g645fFpfMKCNXysEb9xiBeEj5de
2x5sX/0OSx4=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIICUjCCAdegAwIBAgIJAMFD4n5iQ8zoMAoGCCqGSM49BAMCMD4xCzAJBgNVBAYT
Ak5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBF
QyBDQTAeFw0xMzA5MjQxNTQ5NDhaFw0yMzA5MjIxNTQ5NDhaMD4xCzAJBgNVBAYT
Ak5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBF
QyBDQTB2MBAGByqGSM49AgEGBSuBBAAiA2IABMPaKzRBN1gvh1b+/Im6KUNLTuBu
ww5XUzM5WNRStJGVOQsj318XJGJI/BqVKc4sLYfCiFKAr9ZqqyHduNMcbli4yuiy
aY7zQa0pw7RfdadHb9UZKVVpmlM7ILRmFmAzHqOBoDCBnTAdBgNVHQ4EFgQUnW0g
JEkBPyvLeLUZvH4kydv7NnwwbgYDVR0jBGcwZYAUnW0gJEkBPyvLeLUZvH4kydv7
NnyhQqRAMD4xCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UE
AxMTUG9sYXJzc2wgVGVzdCBFQyBDQYIJAMFD4n5iQ8zoMAwGA1UdEwQFMAMBAf8w
CgYIKoZIzj0EAwIDaQAwZgIxAMO0YnNWKJUAfXgSJtJxexn4ipg+kv4znuR50v56
t4d0PCu412mUC6Nnd7izvtE2MgIxAP1nnJQjZ8BWukszFQDG48wxCCyci9qpdSMv
uCjn8pwUOkABXK8Mss90fzCfCEOtIA==

-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB+zCCAYCgAwIBAgIBATAMBggqhkjOPQQDAgUAMD4xCzAJBgNVBAYTAk5MMREw
DwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBFQyBDQTAe
Fw0yMzA5MjIxNTQ5NDlaFw0zMDEyMzEyMzU5NTlaMD4xCzAJBgNVBAYTAk5MMREw
DwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBFQyBDQTB2
MBAGByqGSM49AgEGBSuBBAAiA2IABMPaKzRBN1gvh1b+/Im6KUNLTuBuww5XUzM5
WNRStJGVOQsj318XJGJI/BqVKc4sLYfCiFKAr9ZqqyHduNMcbli4yuiyaY7zQa0p
w7RfdadHb9UZKVVpmlM7ILRmFmAzHqNQME4wDAYDVR0TBAUwAwEB/zAdBgNVHQ4E
FgQUnW0gJEkBPyvLeLUZvH4kydv7NnwwHwYDVR0jBBgwFoAUnW0gJEkBPyvLeLUZ
vH4kydv7NnwwDAYIKoZIzj0EAwIFAANnADBkAjB1ZNdOM7KRJiPo45hP17A1sJSH
qHFPEJbml6KdNevoVZ1HqvP8AoFGcPJRpQVtzC0CMDa7JEqn0dOss8EmW9pVF/N2
+XvzNczj89mWMgPhJJlT+MONQx3LFQO+TMSI9hLdkw==
-----END
CERTIFICATE-----
Camellia-128-ECB Encrypt RFC3713 #1
camellia_encrypt_ecb:"0123456789abcdeffedcba9876543210":"0123456789abcdeffedcba9876543210":"67673138
549669730857065648eabe43":0

Camellia-192-ECB Encrypt RFC3713 #1
camellia_encrypt_ecb:"0123456789abcdeffedcba98765432100011223344556677":"0123456789abcdeffedcba98765
43210":"b4993401b3e996f84ee5cee7d79b09b9":0

Camellia-256-ECB Encrypt RFC3713 #1
camellia_encrypt_ecb:"0123456789abcdeffedcba9876543210001122334455667788 99aabbccddeeff":"0123456789a
bcdeffedcba9876543210":"9acc237dff16d76c20ef7c919e3a7509":0

Camellia-128-ECB Encrypt Perl EVP #1
camellia_encrypt_ecb:"000102030405060708090A0B0C0D0E0F":"00112233445566778899AABBCCDDEEFF":"
77CF412067AF827061352914991954 6F":0

Camellia-192-ECB Encrypt Perl EVP #1
camellia_encrypt_ecb:"000102030405060708090A0B0C0D0E0F1011121314151617":"00112233445566778899A
ABBCCDDEEFF":"B22F3C36B72D31329EEE8ADDC2906C68":0

Camellia-256-ECB Encrypt Perl EVP #1
camellia_encrypt_ecb:"000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F":"0011
2233445566778899AABBCCDDEEFF":"2EDF1F3418D53B88841FC8985FB1ECF2":0

Camellia-128-ECB
Encrypt Perl EVP #1
camellia_encrypt_ecb:"2B7E151628AED2A6ABF7158809CF4F3C":"6BC1BEE22E409F96E93D7E117393172A":
"432FC5DCD628115B7C388D770B270C96":0

Camellia-128-ECB Encrypt Perl EVP #2
camellia_encrypt_ecb:"2B7E151628AED2A6ABF7158809CF4F3C":"AE2D8A571E03AC9C9EB76FAC45AF8E5
1":"0BE1F14023782A22E8384C5ABB7FAB2B":0

Camellia-128-ECB Encrypt Perl EVP #3
camellia_encrypt_ecb:"2B7E151628AED2A6ABF7158809CF4F3C":"30C81C46A35CE411E5FBC1191A0A52EF":"A0A1ABCD1893AB6FE0FE5B65DF5F8636":0

Camellia-128-ECB Encrypt Perl EVP #4
camellia_encrypt_ecb:"2B7E151628AED2A6ABF7158809CF4F3C":"F69F2445DF4F9B17AD2B417BE66C3710":"E61925E0D5DFAA9BB29F815B3076E51A":0

Camellia-192-ECB Encrypt Perl EVP #1
camellia_encrypt_ecb:"8E73B0F7DA0E6452C810F32B809079E562F8EAD2522C6B7B":"6BC1BEE22E409F96E93D7E117393172A":"CCCC6C4E138B45848514D48D0D3439D3":0

Camellia-192-ECB Encrypt Perl EVP #2
camellia_encrypt_ecb:"8E73B0F7DA0E6452C810F32B809079E562F8EAD2522C6B7B":"AE2D8A571E03AC9C9EB76FAC45AF8E51":"5713C62C14B2EC0F8393B6AFD6F5785A":0

Camellia-192-ECB
Encrypt Perl EVP #3
camellia_encrypt_ecb:"8E73B0F7DA0E6452C810F32B809079E562F8EAD2522C6B7B":"30C81C46A35CE411E5FBC1191A0A52EF":"B40ED2B60EB54D09D030CF511FEEF366":0

Camellia-192-ECB Encrypt Perl EVP #4
camellia_encrypt_ecb:"8E73B0F7DA0E6452C810F32B809079E562F8EAD2522C6B7B":"F69F2445DF4F9B17AD2B417BE66C3710":"909DBD95799096748CB27357E73E1D26":0

Camellia-256-ECB Encrypt Perl EVP #1
camellia_encrypt_ecb:"603DEB1015CA71BE2B73AEF0857D77811F352C073B6108D72D9810A30914DFF4":"6BC1BEE22E409F96E93D7E117393172A":"BEFD219B112FA00098919CD101C9CCFA":0

Camellia-256-ECB Encrypt Perl EVP #2
camellia_encrypt_ecb:"603DEB1015CA71BE2B73AEF0857D77811F352C073B6108D72D9810A30914DFF4":"AE2D8A571E03AC9C9EB76FAC45AF8E51":"C91D3A8F1AEA08A9386CF4B66C0169EA":0

Camellia-256-ECB Encrypt Perl EVP #3
camellia_encrypt_ecb:"603DEB1015CA71BE2B73AEF0857D77811F352C073B6108D72D9810A30914DFF4":"30C81C46A35CE411E5FBC1191A0A52EF":"A623D711DC5F25A51BB8A80D56397D28":0

Camellia-256-ECB
Encrypt Perl EVP #4
camellia_encrypt_ecb:"603DEB1015CA71BE2B73AEF0857D77811F352C073B6108D72D9810A30914DFF4":"F69F2445DF4F9B17AD2B417BE66C3710":"7960109FB6DC42947FCFE59EA3C5EB6B":0

Camellia-128-CBC Encrypt Perl EVP #1
camellia_encrypt_cbc:"2B7E151628AED2A6ABF7158809CF4F3C":"000102030405060708090A0B0C0D0E0F":"6BC1BEE22E409F96E93D7E117393172A":"1607CF494B36BBF00DAEB0B503C831AB":0

Camellia-128-CBC Encrypt Perl EVP #2
camellia_encrypt_cbc:"2B7E151628AED2A6ABF7158809CF4F3C":"1607CF494B36BBF00DAEB0B503C831AB

":"AE2D8A571E03AC9C9EB76FAC45AF8E51":"A2F2CF671629EF7840C5A5DFB5074887":0

Camellia-128-CBC Encrypt Perl EVP #3
camellia_encrypt_cbc:"2B7E151628AED2A6ABF7158809CF4F3C":"A2F2CF671629EF7840C5A5DFB5074887":"30C81C46A35CE411E5FBC1191A0A52EF":"0F06165008CF8B8B5A63586362543E54":0

Camellia-128-CBC Encrypt Perl EVP #4
camellia_encrypt_cbc:"2B7E151628AED2A6ABF7158809CF4F3C":"36A84CDAFD5F9A85ADA0F0A993D6D577":"F69F2445DF4F9B17AD2B417BE66C3710":"74C64268CDB8B8FAF5B34E8AF3732980":0

Camellia-192-CBC
Encrypt Perl EVP #1
camellia_encrypt_cbc:"8E73B0F7DA0E6452C810F32B809079E562F8EAD2522C6B7B":"0001020304050607080 90A0B0C0D0E0F":"6BC1BEE22E409F96E93D7E117393172A":"2A4830AB5AC4A1A2405955FD2195CF93":0

Camellia-192-CBC Encrypt Perl EVP #2
camellia_encrypt_cbc:"8E73B0F7DA0E6452C810F32B809079E562F8EAD2522C6B7B":"2A4830AB5AC4A1A2405955FD2195CF93":"AE2D8A571E03AC9C9EB76FAC45AF8E51":"5D5A869BD14CE54264F892A6DD2EC3D5":0

Camellia-192-CBC Encrypt Perl EVP #3
camellia_encrypt_cbc:"8E73B0F7DA0E6452C810F32B809079E562F8EAD2522C6B7B":"5D5A869BD14CE54264F892A6DD2EC3D5":"30C81C46A35CE411E5FBC1191A0A52EF":"37D359C3349836D884E310ADDF68C449":0

Camellia-192-CBC Encrypt Perl EVP #4
camellia_encrypt_cbc:"8E73B0F7DA0E6452C810F32B809079E562F8EAD2522C6B7B":"37D359C3349836D884E310ADDF68C449":"F69F2445DF4F9B17AD2B417BE66C3710":"01FAAA930B4AB9916E9668E1428C6B08":0

Camellia-256-CBC Encrypt Perl EVP #1
camellia_encrypt_cbc:"603DEB1015CA71BE2B73AEF0857D77811F352C073B6108D72D9810A30914DFF4":"0001020304050607080 90A0B0C0D0E0F":"6BC1BEE22E409F96E93D7E117393172A":"E6CFA35FC02B134A4D2C0B6737AC3EDA":0

Camellia-256-CBC
Encrypt Perl EVP #2
camellia_encrypt_cbc:"603DEB1015CA71BE2B73AEF0857D77811F352C073B6108D72D9810A30914DFF4":"E6CFA35FC02B134A4D2C0B6737AC3EDA":"AE2D8A571E03AC9C9EB76FAC45AF8E51":"36CBEB73BD504B4070B1B7DE2B21EB50":0

Camellia-256-CBC Encrypt Perl EVP #3
camellia_encrypt_cbc:"603DEB1015CA71BE2B73AEF0857D77811F352C073B6108D72D9810A30914DFF4":"36CBEB73BD504B4070B1B7DE2B21EB50":"30C81C46A35CE411E5FBC1191A0A52EF":"E31A6055297D96CA3330CDF1B1860A83":0

Camellia-256-CBC Encrypt Perl EVP #4
camellia_encrypt_cbc:"603DEB1015CA71BE2B73AEF0857D77811F352C073B6108D72D9810A30914DFF4":"E

31A6055297D96CA3330CDF1B1860A83":"F69F2445DF4F9B17AD2B417BE66C3710":"5D563F6D1CCCF2360
51C0C5C1C58F28F":0

Camellia-128-CFB128 Encrypt Perl EVP #1
depends_on:MBEDTLS_CIPHER_MODE_CFB
camellia_encrypt_cfb128:"2B7E151628AED2A6ABF7158809CF4F3C":"000102030405060708090A0B0C0D0E0
F":"6BC1BEE22E409F96E93D7E117393172A":"14F7646187817EB586599146B82BD719"

Camellia-128-CFB128
Encrypt Perl EVP #2
depends_on:MBEDTLS_CIPHER_MODE_CFB
camellia_encrypt_cfb128:"2B7E151628AED2A6ABF7158809CF4F3C":"14F7646187817EB586599146B82BD719
":"AE2D8A571E03AC9C9EB76FAC45AF8E51":"A53D28BB82DF741103EA4F921A44880B"

Camellia-128-CFB128 Encrypt Perl EVP #3
depends_on:MBEDTLS_CIPHER_MODE_CFB
camellia_encrypt_cfb128:"2B7E151628AED2A6ABF7158809CF4F3C":"A53D28BB82DF741103EA4F921A4488
0B":"30C81C46A35CE411E5FBC1191A0A52EF":"9C2157A664626D1DEF9EA420FDE69B96"

Camellia-128-CFB128 Encrypt Perl EVP #4
depends_on:MBEDTLS_CIPHER_MODE_CFB
camellia_encrypt_cfb128:"2B7E151628AED2A6ABF7158809CF4F3C":"9C2157A664626D1DEF9EA420FDE69B
96":"F69F2445DF4F9B17AD2B417BE66C3710":"742A25F0542340C7BAEF24CA8482BB09"

Camellia-128-CFB128 Decrypt Perl EVP #1
depends_on:MBEDTLS_CIPHER_MODE_CFB
camellia_decrypt_cfb128:"2B7E151628AED2A6ABF7158809CF4F3C":"000102030405060708090A0B0C0D0E0
F":"6BC1BEE22E409F96E93D7E117393172A":"14F7646187817EB586599146B82BD719"

Camellia-128-CFB128
Decrypt Perl EVP #2
depends_on:MBEDTLS_CIPHER_MODE_CFB
camellia_decrypt_cfb128:"2B7E151628AED2A6ABF7158809CF4F3C":"14F7646187817EB586599146B82BD719
":"AE2D8A571E03AC9C9EB76FAC45AF8E51":"A53D28BB82DF741103EA4F921A44880B"

Camellia-128-CFB128 Decrypt Perl EVP #3
depends_on:MBEDTLS_CIPHER_MODE_CFB
camellia_decrypt_cfb128:"2B7E151628AED2A6ABF7158809CF4F3C":"A53D28BB82DF741103EA4F921A4488
0B":"30C81C46A35CE411E5FBC1191A0A52EF":"9C2157A664626D1DEF9EA420FDE69B96"

Camellia-128-CFB128 Decrypt Perl EVP #4
depends_on:MBEDTLS_CIPHER_MODE_CFB
camellia_decrypt_cfb128:"2B7E151628AED2A6ABF7158809CF4F3C":"9C2157A664626D1DEF9EA420FDE69B
96":"F69F2445DF4F9B17AD2B417BE66C3710":"742A25F0542340C7BAEF24CA8482BB09"

Camellia-192-CFB128 Encrypt Perl EVP #1
depends_on:MBEDTLS_CIPHER_MODE_CFB
camellia_encrypt_cfb128:"8E73B0F7DA0E6452C810F32B809079E562F8EAD2522C6B7B":"0001020304050607

08090A0B0C0D0E0F":"6BC1BEE22E409F96E93D7E117393172A":"C832BB9780677DAA82D9B6860DCD565E"

Camellia-192-CFB128
Encrypt Perl EVP #2
depends_on:MBEDTLS_CIPHER_MODE_CFB
camellia_encrypt_cfb128:"8E73B0F7DA0E6452C810F32B809079E562F8EAD2522C6B7B":"C832BB9780677DAA82D9B6860DCD565E":"AE2D8A571E03AC9C9EB76FAC45AF8E51":"86F8491627906D780C7A6D46EA331F98"

Camellia-192-CFB128 Encrypt Perl EVP #3
depends_on:MBEDTLS_CIPHER_MODE_CFB
camellia_encrypt_cfb128:"8E73B0F7DA0E6452C810F32B809079E562F8EAD2522C6B7B":"86F8491627906D780C7A6D46EA331F98":"30C81C46A35CE411E5FBC1191A0A52EF":"69511CCE594CF710CB98BB63D7221F01"

Camellia-192-CFB128 Encrypt Perl EVP #4
depends_on:MBEDTLS_CIPHER_MODE_CFB
camellia_encrypt_cfb128:"8E73B0F7DA0E6452C810F32B809079E562F8EAD2522C6B7B":"69511CCE594CF710CB98BB63D7221F01":"F69F2445DF4F9B17AD2B417BE66C3710":"D5B5378A3ABED55803F25565D8907B84"

Camellia-192-CFB128 Decrypt Perl EVP #1
depends_on:MBEDTLS_CIPHER_MODE_CFB
camellia_decrypt_cfb128:"8E73B0F7DA0E6452C810F32B809079E562F8EAD2522C6B7B":"0001020304050607
08090A0B0C0D0E0F":"6BC1BEE22E409F96E93D7E117393172A":"C832BB9780677DAA82D9B6860DCD565E"

Camellia-192-CFB128
Decrypt Perl EVP #2
depends_on:MBEDTLS_CIPHER_MODE_CFB
camellia_decrypt_cfb128:"8E73B0F7DA0E6452C810F32B809079E562F8EAD2522C6B7B":"C832BB9780677DAA82D9B6860DCD565E":"AE2D8A571E03AC9C9EB76FAC45AF8E51":"86F8491627906D780C7A6D46EA331F98"

Camellia-192-CFB128 Decrypt Perl EVP #3
depends_on:MBEDTLS_CIPHER_MODE_CFB
camellia_decrypt_cfb128:"8E73B0F7DA0E6452C810F32B809079E562F8EAD2522C6B7B":"86F8491627906D780C7A6D46EA331F98":"30C81C46A35CE411E5FBC1191A0A52EF":"69511CCE594CF710CB98BB63D7221F01"

Camellia-192-CFB128 Decrypt Perl EVP #4
depends_on:MBEDTLS_CIPHER_MODE_CFB
camellia_decrypt_cfb128:"8E73B0F7DA0E6452C810F32B809079E562F8EAD2522C6B7B":"69511CCE594CF710CB98BB63D7221F01":"F69F2445DF4F9B17AD2B417BE66C3710":"D5B5378A3ABED55803F25565D8907B84"

Camellia-256-CFB128 Encrypt Perl EVP #1

depends_on:MBEDTLS_CIPHER_MODE_CFB
camellia_encrypt_cfb128:"603DEB1015CA71BE2B73AEF0857D77811F352C073B6108D72D9810A30914DFF4"
:"000102030405060708090A0B0C0D0E0F":"6BC1BEE22E409F96E93D7E117393172A":"CF6107BB0CEA7D7F
B1BD31F5E7B06C93"

Camellia-256-CFB128
Encrypt Perl EVP #2
depends_on:MBEDTLS_CIPHER_MODE_CFB
camellia_encrypt_cfb128:"603DEB1015CA71BE2B73AEF0857D77811F352C073B6108D72D9810A30914DFF4"
:"CF6107BB0CEA7D7FB1BD31F5E7B06C93":"AE2D8A571E03AC9C9EB76FAC45AF8E51":"89BEDB4CCDD
864EA11BA4CBE849B5E2B"

Camellia-256-CFB128 Encrypt Perl EVP #3
depends_on:MBEDTLS_CIPHER_MODE_CFB
camellia_encrypt_cfb128:"603DEB1015CA71BE2B73AEF0857D77811F352C073B6108D72D9810A30914DFF4"
:"89BEDB4CCDD864EA11BA4CBE849B5E2B":"30C81C46A35CE411E5FBC1191A0A52EF":"555FC3F34BDD
2D54C62D9E3BF338C1C4"

Camellia-256-CFB128 Encrypt Perl EVP #4
depends_on:MBEDTLS_CIPHER_MODE_CFB
camellia_encrypt_cfb128:"603DEB1015CA71BE2B73AEF0857D77811F352C073B6108D72D9810A30914DFF4"
:"555FC3F34BDD2D54C62D9E3BF338C1C4":"F69F2445DF4F9B17AD2B417BE66C3710":"5953ADCE14DB8
C7F39F1BD39F359BFFA"

Camellia-256-CFB128 Decrypt Perl EVP #1
depends_on:MBEDTLS_CIPHER_MODE_CFB
camellia_decrypt_cfb128:"603DEB1015CA71BE2B73AEF0857D77811F352C073B6108D72D9810A30914DFF4"
:"000102030405060708090A0B0C0D0E0F":"6BC1BEE22E409F96E93D7E117393172A":"CF6107BB0CEA7D7F
B1BD31F5E7B06C93"

Camellia-256-CFB128
Decrypt Perl EVP #2
depends_on:MBEDTLS_CIPHER_MODE_CFB
camellia_decrypt_cfb128:"603DEB1015CA71BE2B73AEF0857D77811F352C073B6108D72D9810A30914DFF4"
:"CF6107BB0CEA7D7FB1BD31F5E7B06C93":"AE2D8A571E03AC9C9EB76FAC45AF8E51":"89BEDB4CCDD
864EA11BA4CBE849B5E2B"

Camellia-256-CFB128 Decrypt Perl EVP #3
depends_on:MBEDTLS_CIPHER_MODE_CFB
camellia_decrypt_cfb128:"603DEB1015CA71BE2B73AEF0857D77811F352C073B6108D72D9810A30914DFF4"
:"89BEDB4CCDD864EA11BA4CBE849B5E2B":"30C81C46A35CE411E5FBC1191A0A52EF":"555FC3F34BDD
2D54C62D9E3BF338C1C4"

Camellia-256-CFB128 Decrypt Perl EVP #4
depends_on:MBEDTLS_CIPHER_MODE_CFB
camellia_decrypt_cfb128:"603DEB1015CA71BE2B73AEF0857D77811F352C073B6108D72D9810A30914DFF4"
:"555FC3F34BDD2D54C62D9E3BF338C1C4":"F69F2445DF4F9B17AD2B417BE66C3710":"5953ADCE14DB8
C7F39F1BD39F359BFFA"

Camellia-ECB
Encrypt (Invalid key length)
camellia_encrypt_ecb:"0123456789abcdeffedcba98765432":"0123456789abcdeffedcba9876543210":"6767313854
9669730857065648eabe43":MBEDTLS_ERR_CAMELLIA_INVALID_KEY_LENGTH

Camellia-ECB Decrypt (Invalid key length)
camellia_decrypt_ecb:"0123456789abcdeffedcba98765432":"0123456789abcdeffedcba9876543210":"6767313854
9669730857065648eabe43":MBEDTLS_ERR_CAMELLIA_INVALID_KEY_LENGTH

Camellia-256-CBC Encrypt (Invalid input length)
camellia_encrypt_cbc:"0000000000000000000000000000000000000000000000000000000000000000":"00000000
00000000000000000000000":"ffffffffffffffe000000000000000":"":MBEDTLS_ERR_CAMELLIA_INVALID_IN
PUT_LENGTH

Camellia-256-CBC Decrypt (Invalid input length)
camellia_decrypt_cbc:"0000000000000000000000000000000000000000000000000000000000000000":"00000000
00000000000000000000000":"623a52fcea5d443e48d9181ab32c74":"":MBEDTLS_ERR_CAMELLIA_INVALID
_INPUT_LENGTH

Camellia Selftest
depends_on:MBEDTLS_SELF_TEST
camellia_selftest:
-----BEGIN CERTIFICATE-----
MIIBoTCCAUWgAwIBAgIBXDAMBggqhkjOPQQDAgUAMDExDzANBgNVBAMTBlJvb3Qg
OTERMA8GA1UEChMIbWJlZCBUTFMxCzAJBgNVBAYTAlVLMB4XDTAxMDEwMTAwMDAw
MFoXDTMwMTIzMTIzNTk1OVowMDEOMAwGA1UEAxMFRUUgOTIxETAPBgNVBAoTCG1i
ZWQgVExTMQswCQYDVQQGEwJVSzBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABC9E
tK1pE8Ei8vgScunyjx50C+qDsQS8D2RhGHC4VkE2yyiFxJA/ynhoeXTKZsHuEWI9
CfOSvk0RrTWf9nr0pTGjTTBLMAkGA1UdEwQCMAAwHQYDVR0OBBYEFLqsN52tAf1k
XlzxQmdD5qG6Sy6PMB8GA1UdIwQYMBaAFFvNWtwDF12PSLQMSq9MZPwXftuLMAwG
CCqGSM49BAMCBQADSAAwRQIgXlfKqhkhXgK112Eycl+Z5NHM+6aqXE7i9j7IyGfk
ikICIQDBYNGbpSx82XG+IS/h4AWNTa4Hs6rmWvQDWJum7NrzMQ==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIBpTCCAUmgAwIBAgIBUTAMBggqhkjOPQQDAgUAMDExDzANBgNVBAMTBlJvb3Qg
ODERMA8GA1UEChMIbWJlZCBUTFMxCzAJBgNVBAYTAlVLMB4XDTAxMDEwMTAwMDAw
MFoXDTMwMTIzMTIzNTk1OVowMTEPMA0GA1UEAxMGUm9vdCA4MREwDwYDVQQKEwht
YmVkIFRMUzELMAkGA1UEBhMCVUswWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAT1
GuTQ9vgf2l3oLM25r78cvIAQqE02GzQGjp/WWw3CysEwTwNEuZGhRiD5lDmkbUGW
UNxv/7uJjy7k3K3fDNdko1AwTjAMBgNVHRMEBTADAQH/MB0GA1UdDgQWBBTHFA2h
Au0tPnzeYnLcmlTQj4FAajAfBgNVHSMEGDAWgBTHFA2hAu0tPnzeYnLcmlTQj4FA
ajAMBggqhkjOPQQDAgUAA0gAMEUCIH7Z/HNb/Pwbs40iNll1a9gmgAbYOgdlVPWo
nSdcb7cZAiEAlhVb6CdBXsjOfAWWEET/QP74z608PKFccCIFPCDLkxo=
-----END CERTIFICATE-----
[int]
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid:always,issuer:always

basicConstraints = CA:true
Cipher list
mbedtls_cipher_list:

Cipher null/uninitialised arguments
cipher_null_args:

Set padding with AES-CBC
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
set_padding:MBEDTLS_CIPHER_AES_128_CBC:MBEDTLS_PADDING_PKCS7:0

Set padding with AES-CFB
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CFB
set_padding:MBEDTLS_CIPHER_AES_128_CFB128:MBEDTLS_PADDING_PKCS7:MBEDTLS_ERR_CIPHER_BAD_INPUT_DATA

Set padding with AES-CTR
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CTR
set_padding:MBEDTLS_CIPHER_AES_128_CTR:MBEDTLS_PADDING_PKCS7:MBEDTLS_ERR_CIPHER_BAD_INPUT_DATA

Set padding with CAMELLIA-CBC
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
set_padding:MBEDTLS_CIPHER_CAMELLIA_128_CBC:MBEDTLS_PADDING_PKCS7:0

Set padding with CAMELLIA-CFB
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CFB
set_padding:MBEDTLS_CIPHER_CAMELLIA_128_CFB128:MBEDTLS_PADDING_PKCS7:MBEDTLS_ERR_CIPHER_BAD_INPUT_DATA

Set padding with CAMELLIA-CTR
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CTR
set_padding:MBEDTLS_CIPHER_CAMELLIA_128_CTR:MBEDTLS_PADDING_PKCS7:MBEDTLS_ERR_CIPHER_BAD_INPUT_DATA

Set
padding with DES-CBC
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
set_padding:MBEDTLS_CIPHER_DES_CBC:MBEDTLS_PADDING_PKCS7:0

Set padding with BLOWFISH-CBC
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
set_padding:MBEDTLS_CIPHER_BLOWFISH_CBC:MBEDTLS_PADDING_PKCS7:0

Set padding with BLOWFISH-CFB
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CFB

set_padding:MBEDTLS_CIPHER_BLOWFISH_CFB64:MBEDTLS_PADDING_PKCS7:MBEDTLS_ERR_CIPHER_BAD_INPUT_DATA

Set padding with BLOWFISH-CTR
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CTR
set_padding:MBEDTLS_CIPHER_BLOWFISH_CTR:MBEDTLS_PADDING_PKCS7:MBEDTLS_ERR_CIPHER_BAD_INPUT_DATA

Set padding with NULL
depends_on:MBEDTLS_CIPHER_NULL_CIPHER
set_padding:MBEDTLS_CIPHER_NULL:MBEDTLS_PADDING_PKCS7:MBEDTLS_ERR_CIPHER_BAD_INPUT_DATA

Set
non-existent padding with AES-CBC
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC
set_padding:MBEDTLS_CIPHER_AES_128_CBC:-1:MBEDTLS_ERR_CIPHER_FEATURE_UNAVAILABLE

Set non-existent padding with CAMELLIA-CBC
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC
set_padding:MBEDTLS_CIPHER_CAMELLIA_128_CBC:-1:MBEDTLS_ERR_CIPHER_FEATURE_UNAVAILABLE

Set non-existent padding with DES-CBC
depends_on:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC
set_padding:MBEDTLS_CIPHER_DES_CBC:-1:MBEDTLS_ERR_CIPHER_FEATURE_UNAVAILABLE

Set non-existent padding with BLOWFISH-CBC
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC
set_padding:MBEDTLS_CIPHER_BLOWFISH_CBC:-1:MBEDTLS_ERR_CIPHER_FEATURE_UNAVAILABLE

Check PKCS padding #1 (correct)
depends_on:MBEDTLS_CIPHER_PADDING_PKCS7
check_padding:MBEDTLS_PADDING_PKCS7:"DABBAD0004040404":0:4

Check PKCS padding #2 (correct)
depends_on:MBEDTLS_CIPHER_PADDING_PKCS7
check_padding:MBEDTLS_PADDING_PKCS7:"DABBAD0001":0:4

Check PKCS padding #3 (correct)
depends_on:MBEDTLS_CIPHER_PADDING_PKCS7
check_padding:MBEDTLS_PADDING_PKCS7:"DABBAD000101":0:5

Check
PKCS padding #4 (correct)
depends_on:MBEDTLS_CIPHER_PADDING_PKCS7
check_padding:MBEDTLS_PADDING_PKCS7:"030303":0:0

Check PKCS padding #5 (null padding)
depends_on:MBEDTLS_CIPHER_PADDING_PKCS7
check_padding:MBEDTLS_PADDING_PKCS7:"DABBAD0000":MBEDTLS_ERR_CIPHER_INVALID_PADDING:0

Check PKCS padding #6 (too few padding bytes)
depends_on:MBEDTLS_CIPHER_PADDING_PKCS7
check_padding:MBEDTLS_PADDING_PKCS7:"DABBAD0002":MBEDTLS_ERR_CIPHER_INVALID_PADDING:0

Check PKCS padding #7 (non-uniform padding bytes #1)
depends_on:MBEDTLS_CIPHER_PADDING_PKCS7
check_padding:MBEDTLS_PADDING_PKCS7:"DABBAD00030203":MBEDTLS_ERR_CIPHER_INVALID_PADDING:0

Check PKCS padding #7 (non-uniform padding bytes #2)
depends_on:MBEDTLS_CIPHER_PADDING_PKCS7
check_padding:MBEDTLS_PADDING_PKCS7:"DABBAD00030103":MBEDTLS_ERR_CIPHER_INVALID_PADDING:0

Check PKCS padding #7 (non-uniform padding bytes #3)
depends_on:MBEDTLS_CIPHER_PADDING_PKCS7
check_padding:MBEDTLS_PADDING_PKCS7:"DABBAD00030703":MBEDTLS_ERR_CIPHER_INVALID_PADDING:0

Check
PKCS padding #7 (non-uniform padding bytes #4)
depends_on:MBEDTLS_CIPHER_PADDING_PKCS7
check_padding:MBEDTLS_PADDING_PKCS7:"DABBAD00030b03":MBEDTLS_ERR_CIPHER_INVALID_PADDING:0

Check PKCS padding #7 (non-uniform padding bytes #5)
depends_on:MBEDTLS_CIPHER_PADDING_PKCS7
check_padding:MBEDTLS_PADDING_PKCS7:"DABBAD00031303":MBEDTLS_ERR_CIPHER_INVALID_PADDING:0

Check PKCS padding #7 (non-uniform padding bytes #6)
depends_on:MBEDTLS_CIPHER_PADDING_PKCS7
check_padding:MBEDTLS_PADDING_PKCS7:"DABBAD00032303":MBEDTLS_ERR_CIPHER_INVALID_PADDING:0

Check PKCS padding #7 (non-uniform padding bytes #7)
depends_on:MBEDTLS_CIPHER_PADDING_PKCS7
check_padding:MBEDTLS_PADDING_PKCS7:"DABBAD00034203":MBEDTLS_ERR_CIPHER_INVALID_PADDING:0

Check PKCS padding #7 (non-uniform padding bytes #8)

depends_on:MBEDTLS_CIPHER_PADDING_PKCS7
check_padding:MBEDTLS_PADDING_PKCS7:"DABBAD00038303":MBEDTLS_ERR_CIPHER_INVALID_PADDING:0

Check
PKCS padding #7 (non-uniform padding bytes #9)
depends_on:MBEDTLS_CIPHER_PADDING_PKCS7
check_padding:MBEDTLS_PADDING_PKCS7:"DABBAD00020303":MBEDTLS_ERR_CIPHER_INVALID_PADDING:0

Check PKCS padding #7 (non-uniform padding bytes #10)
depends_on:MBEDTLS_CIPHER_PADDING_PKCS7
check_padding:MBEDTLS_PADDING_PKCS7:"DABBAD00010303":MBEDTLS_ERR_CIPHER_INVALID_PADDING:0

Check PKCS padding #7 (non-uniform padding bytes #11)
depends_on:MBEDTLS_CIPHER_PADDING_PKCS7
check_padding:MBEDTLS_PADDING_PKCS7:"DABBAD00070303":MBEDTLS_ERR_CIPHER_INVALID_PADDING:0

Check PKCS padding #7 (non-uniform padding bytes #12)
depends_on:MBEDTLS_CIPHER_PADDING_PKCS7
check_padding:MBEDTLS_PADDING_PKCS7:"DABBAD000b0303":MBEDTLS_ERR_CIPHER_INVALID_PADDING:0

Check PKCS padding #7 (non-uniform padding bytes #13)
depends_on:MBEDTLS_CIPHER_PADDING_PKCS7
check_padding:MBEDTLS_PADDING_PKCS7:"DABBAD00130303":MBEDTLS_ERR_CIPHER_INVALID_PADDING:0

Check PKCS padding #7 (non-uniform padding bytes #14)
depends_on:MBEDTLS_CIPHER_PADDING_PKCS7
check_padding:MBEDTLS_PADDING_PKCS7:"DABBAD00230303":MBEDTLS_ERR_CIPHER_INVALID_PADDING:0

Check
PKCS padding #7 (non-uniform padding bytes #15)
depends_on:MBEDTLS_CIPHER_PADDING_PKCS7
check_padding:MBEDTLS_PADDING_PKCS7:"DABBAD00420303":MBEDTLS_ERR_CIPHER_INVALID_PADDING:0

Check PKCS padding #7 (non-uniform padding bytes #16)
depends_on:MBEDTLS_CIPHER_PADDING_PKCS7
check_padding:MBEDTLS_PADDING_PKCS7:"DABBAD00830303":MBEDTLS_ERR_CIPHER_INVALID_PADDING:0

Check PKCS padding #8 (overlong)
depends_on:MBEDTLS_CIPHER_PADDING_PKCS7

check_padding:MBEDTLS_PADDING_PKCS7:"040404":MBEDTLS_ERR_CIPHER_INVALID_PADDING:0

Check one and zeros padding #1 (correct)
depends_on:MBEDTLS_CIPHER_PADDING_ONE_AND_ZEROS
check_padding:MBEDTLS_PADDING_ONE_AND_ZEROS:"DABBAD0080":0:4

Check one and zeros padding #2 (correct)
depends_on:MBEDTLS_CIPHER_PADDING_ONE_AND_ZEROS
check_padding:MBEDTLS_PADDING_ONE_AND_ZEROS:"DABBAD008000":0:4

Check one and zeros padding #3 (correct)
depends_on:MBEDTLS_CIPHER_PADDING_ONE_AND_ZEROS
check_padding:MBEDTLS_PADDING_ONE_AND_ZEROS:"DABBAD00800000":0:4

Check
one and zeros padding #4 (correct)
depends_on:MBEDTLS_CIPHER_PADDING_ONE_AND_ZEROS
check_padding:MBEDTLS_PADDING_ONE_AND_ZEROS:"DABBAD00808000":0:5

Check one and zeros padding #5 (correct)
depends_on:MBEDTLS_CIPHER_PADDING_ONE_AND_ZEROS
check_padding:MBEDTLS_PADDING_ONE_AND_ZEROS:"800000":0:0

Check one and zeros padding #6 (missing one)
depends_on:MBEDTLS_CIPHER_PADDING_ONE_AND_ZEROS
check_padding:MBEDTLS_PADDING_ONE_AND_ZEROS:"DABBAD0000":MBEDTLS_ERR_CIPHER_INVALID_PADDING:4

Check one and zeros padding #7 (overlong)
depends_on:MBEDTLS_CIPHER_PADDING_ONE_AND_ZEROS
check_padding:MBEDTLS_PADDING_ONE_AND_ZEROS:"0000000000":MBEDTLS_ERR_CIPHER_INVALID_PADDING:4

Check zeros and len padding #1 (correct)
depends_on:MBEDTLS_CIPHER_PADDING_ZEROS_AND_LEN
check_padding:MBEDTLS_PADDING_ZEROS_AND_LEN:"DABBAD0001":0:4

Check zeros and len padding #2 (correct)
depends_on:MBEDTLS_CIPHER_PADDING_ZEROS_AND_LEN
check_padding:MBEDTLS_PADDING_ZEROS_AND_LEN:"DABBAD000002":0:4

Check
zeros and len padding #3 (correct)
depends_on:MBEDTLS_CIPHER_PADDING_ZEROS_AND_LEN
check_padding:MBEDTLS_PADDING_ZEROS_AND_LEN:"DABBAD000003":0:3

Check zeros and len padding #4 (correct)
depends_on:MBEDTLS_CIPHER_PADDING_ZEROS_AND_LEN

check_padding:MBEDTLS_PADDING_ZEROS_AND_LEN:"000003":0:0

Check zeros and len padding #5 (overlong)
depends_on:MBEDTLS_CIPHER_PADDING_ZEROS_AND_LEN
check_padding:MBEDTLS_PADDING_ZEROS_AND_LEN:"000004":MBEDTLS_ERR_CIPHER_INVALID_PADDING:0

Check zeros and len padding #6 (not enough zeros)
depends_on:MBEDTLS_CIPHER_PADDING_ZEROS_AND_LEN
check_padding:MBEDTLS_PADDING_ZEROS_AND_LEN:"DABBAD000004":MBEDTLS_ERR_CIPHER_INVALID_PADDING:0

Check zeros padding #1 (correct)
depends_on:MBEDTLS_CIPHER_PADDING_ZEROS
check_padding:MBEDTLS_PADDING_ZEROS:"DABBAD00":0:3

Check zeros padding #2 (correct)
depends_on:MBEDTLS_CIPHER_PADDING_ZEROS
check_padding:MBEDTLS_PADDING_ZEROS:"DABBAD0000":0:3

Check
zeros padding #3 (correct)
depends_on:MBEDTLS_CIPHER_PADDING_ZEROS
check_padding:MBEDTLS_PADDING_ZEROS:"DABBAD":0:3

Check zeros padding #4 (correct)
depends_on:MBEDTLS_CIPHER_PADDING_ZEROS
check_padding:MBEDTLS_PADDING_ZEROS:"000000":0:0

Check no padding #1 (correct by definition)
check_padding:MBEDTLS_PADDING_NONE:"DABBAD00":0:4

Check no padding #2 (correct by definition)
check_padding:MBEDTLS_PADDING_NONE:"DABBAD0001":0:5

Check no padding #3 (correct by definition)
check_padding:MBEDTLS_PADDING_NONE:"":0:0
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTQwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTUwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQlKUiMoSss
/hsTasedqdB2BCOGJhTt0hgUGeUnWNZ1svO4yn0GkFHZ08++fl2MKqjpj+VXq0JS
FFyGUOgmgi3Ho4GJMIGGMB0GA1UdDgQWBBR1mXlrdW5rx1VnqMMnUBXo0WWGWjBX
BgNVHSMEUDBOgBRNsJB++ccSBmbCCKBxi4CjXROBk6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTEzggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAKYOIo+fdCQRqpH4LN8qUK1aKzKmWGxS
fGzEEkg/29bMAiAl95cmucoCDMq2Ab8Coc0dEqyJ6+rAPMLBCbGawyiW6A==

-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDWzCCAhKgAwIBAgIBGTA+BgkqhkiG9w0BAQowMaANMAsGCWCGSAFlAwQCAqEa
MBgGCSqGSIb3DQEBCDALBglghkgBZQMEAgKiBAICAM4wOzELMAkGA1UEBhMCTkwx
ETAPBgNVBAoTCFBvbGFyU1NMMRkwFwYDVQQDExBQb2xhclNTTCBUZXN0IENBMB4X
DTE0MDEyMDEzNTc1OFoXDTI0MDExODEzNTc1OFowNDELMAkGA1UEBhMCTkwxETAP
BgNVBAoTCFBvbGFyU1NMMRIwEAYDVQQDEwlsb2NhbGhvc3QwgZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBAN0Rip+ZurBoyirqO2ptWZftTslU5A3uzqB9oB6q6A7C
uxNA24oSjokTJKXF9frY9ZDXyMrLxf6THa/aEiNzUnlGGrqgVyt2FjGzqK/nOJsI
i2OZOgol7kXSGFi6uZMa7dRYmmMbN/z3FAifhWVJ81kybdHg6G3eUu1mtKkL2kCV
AgMBAAGjgZIwgY8wCQYDVR0TBAIwADAdBgNVHQ4EFgQU7vPH9R8VpU1HicHTImOy
36fOvVEwYwYDVR0jBFwwWoAUtFrkpbPe0lL2udWmlQ/rPrzH/f+hP6Q9MDsxCzAJ
BgNVBAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEZMBcGA1UEAxMQUG9sYXJTU0wg
VGVzdCBDQYIBADA+BgkqhkiG9w0BAQowMaANMAsGCWCGSAFlAwQCAqEaMBgGCSqG
SIb3DQEBCDALBglghkgBZQMEAgKiBAICAM4DggEBABf8Gyq2VYuN1EBW1nOapDQp
B/KuafNW2GEJ7FmQKNyA7MIj1Yqo2MtJ6/OQojRQ3F5rnO4yjmvIPsXeQaMxJBiI
aaoAlLpH++F+oXMq/0aS0WSZrSLrsh2Fpay9cBDGwek2rDOX9kM+ZcPzGitVwWKX
TnOW22hpcl7u95CpZH+JZTcto5nL3tTyV9pIy+tSKQQfjPB+G0TAZCsOkbCGPLug
qdjvqFQwOf15VxQMj7NRiXjlqJvsx+I7B2AIhrs4DzQMEyiWq9S/PzpQuFU5v/Kg
s2iMLJ5ygv5aN3PYqGlE1ZmvgyRp5h/LaTGI2L6lzRTnecOhtPv30N2tyaDAEfo=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTQwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTUwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQlKUiMoSss
/hsTasedqdB2BCOGJhTt0hgUGeUnWNZ1svO4yn0GkFHZ08++fl2MKqjpj+VXq0JS
FFyGUOgmgi3Ho4GJMIGGMB0GA1UdDgQWBBR1mXlrdW5rx1VnqMMnUBXo0WWGWjBX
BgNVHSMEUDBOgBRNsJB++ccSBmbCCKBxi4CjXROBk6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTEzggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAKYOIo+fdCQRqpH4LN8qUK1aKzKmWGxS
fGzEEkg/29bMAiAl95cmucoCDMq2Ab8Coc0dEqyJ6+rAPMLBCbGawyiW6A==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTMwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTQwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATRMZN0RHzP
donNmZuq9XPhzvQ52TaokxT39qpQtlFyvUuEGKrLoNvdcpARaA0rGput6RLAQOVU
iNVlJ3Ipj789o4GJMIGGMB0GA1UdDgQWBBRNsJB++ccSBmbCCKBxi4CjXROBkzBX
BgNVHSMEUDBOgBTmVnUSF2MYws/nCMv7b1wJVkDmqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTEyggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgVfuLpjp08AaxKWf6cuZUUCRd7CojSS1I
71hzeUyFS+sCIQDNJI6P/pBbiHgTaGlBAgfcEfmxmbY0n4xZndtxIkmyVA==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----

MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTIwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTMwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATrkzCJLznh
lhnsv1RXB9kfeaD+cIruPQ0cItBDGpdvD8xbBVvQci4+RG2RVUCSWRhkFYjSsUSM
0QHMQnBFlhw2o4GJMIGGMB0GA1UdDgQWBBTmVnUSF2MYwws/nCMv7b1wJVkDmjBX
BgNVHSMEUDBOgBTZTtbi+j0Sm/Zs/+gTkWdASpQzfqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTExggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgWsm+rHJgwUEyNm8EKbEds5yurpp5/3y5
PsvXJVDqxogCIQDUP0Jcl3A907CE2tPVXSgD6LQ6CPu19mixemPw60yijA==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTEwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTIwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATDE9LPlLPc
gZ3b0BchR/AkhNEP9HAavwYadJIyzoPo5edCVnboQH786jsZwZNZoC0gHDAhCmGc
IfRenISAoVuPo4GJMIGGMB0GA1UdDgQWBBTZTtbi+j0Sm/Zs/+gTkWdASpQzfjBX
BgNVHSMEUDBOgBSOSt6ePyMRT6PGMaIi7FqNX9MKtKEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTEwggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgYYF5AnRV7eh2hLD5Dz//pceMTKz9Ls46
E6DxvbfDHikCIFttlGrOCZVyS4ocsjuKIELVUX5qfygI0sn4kU3qCTs2
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTAwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATZwR+WK6NB
F/7riFdN63c8hjYddZRR4lrzVNPwiBQxnnxwpPyrD9A6aPPmLc6SqGOJW4ZGVCco
IBze9RJVeiB9o4GJMIGGMB0GA1UdDgQWBBSOSt6ePyMRT6PGMaIi7FqNX9MKtDBX
BgNVHSMEUDBOgBQtxZSLJAkEz+2RKMQexM6EtsfgcqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA5ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgN//NqM0FrkrMjmxoeCY9DgxkH2R6sQ4d
NgtwCZAIqEICIBs4vupaVcuvni9tltbP26wi7c0FR+blZuo5DPIA3SVe
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDkwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTAwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAR6jlGKbJd5
hiDxN789gkOcwpyHI9wRwCrADAOwOkMePBPRlwGdm7mw7Z/EAmu26zRm/hcyrs4M
qk2LabDjPI9Xo4GJMIGGMB0GA1UdDgQWBBQtxZSLJAkEz+2RKMQexM6EtsfgcjBX
BgNVHSMEUDBOgBT6gyXHzPIPYc1Vr1aGiLLeMh4HpqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA4ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgP7S8vFstfUBdNe6ym5GYG5Q+aBVEKqRs
fVW7HNUktSYCIQDo6Jua6o/DJbrpq4qYWq5gv4yGyzPTN+3IaKrEICdaaw==

-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDgwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDkwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAR7ZB16+t6E
sfahGyKUGJW5mezkzjdaYvc4lbJaKNRwFRfc3F/fmNOSsUFSg/F0N+vUE+doKiPC
8wRwLzvm4s+5o4GJMIGGMB0GA1UdDgQWBBT6gyXHzPIPYc1Vr1aGiLLeMh4HpjBX
BgNVHSMEUDBOgBS40mLt93U8Sh8ZGiDVAhRSiBPcXqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA3ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgO4el1ZPhlIli/qNR2SIEiuvs5Mmy868i
N2Rv5X/VxIECIA/8rUALQxW38XSdBVX3e/jzu7ju47n1YwEqD9K9WdVv
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDcwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDgwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAARpQeQ/YGQj
nl7Szo6WStJ1u7xunTL5jBkXH8aAVSm0qiX4AD/7YPxa5EnGzZdLTn25vQVnfQAG
pMx8P1lYiGYCo4GJMIGGMB0GA1UdDgQWBBS40mLt93U8Sh8ZGiDVAhRSiBPcXjBX
BgNVHSMEUDBOgBREq5J3toJPxZ3O+ssJ5vkkU0RJE6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA2ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhANwGf+F4a+kmXWz8UjSpRkaToTV6EFWw
/Tjzj0tQhDoAAiEA19RxeWOVBBpM6LOHg6v5Lf54YN1snkLf+sEXyZCuWQQ=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDYwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDcwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASNOj4d4MEA
7p/3miijqG4ToE4opKPAm+3BTIGrJTYT14++TSiUICl0ASXj+xeUcLMIaXTN042s
LsHxpShzQaL0o4GJMIGGMB0GA1UdDgQWBBREq5J3toJPxZ3O+ssJ5vkkU0RJEzBX
BgNVHSMEUDBOgBSjovYaC/m6Li9Tp0V9iZRs9267Q6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA1ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAKGcf+c442c/XiwubbaiQvsoZ7EoVxuM
oKmia0gPyBNkAiEA83asjJ5FDXQuLyZpczviXrbmqgCPOfYadtvkc0cxMis=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDUwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDYwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASA9qWoAUHr
nn+3kxyNrjPJk82WDLimW21RN51uxpobadv8YgGEDRdP+Ok+uRqQSUsA6ZXfF3iG
r2GjfQ3wMDH8o4GJMIGGMB0GA1UdDgQWBBSjovYaC/m6Li9Tp0V9iZRs9267QzBX
BgNVHSMEUDBOgBTXh06MAV9S4l4lG1TKOrKRBh4qn6EzpDEwLzELMAkGA1UEBhMC

VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA0ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgcjZNFWJtlDmoPZbAxqsGczRYK0lfPgu6
g1H7pp0ce+wCIDj9BRZM2OB9EF0e+MDKGjyZGfvfrL6Ir47x/KrM6H8T
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDQwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDUwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQEdT0OFf5G
UcrgX2XllCyJzP94NZ464GsgB6psNLsDeL+j7AU+oJy7VLvW/lHh3ODgl08Z9bhq
LFBmNjnHbm8Qo4GJMIGGMB0GA1UdDgQWBBTXh06MAV9S4l4lG1TKOrKRBh4qnzBX
BgNVHSMEUDBOgBQox4F1NsZunlsduoGvzIgRSYfB36EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAzggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAIW++zqDZlLLUk/emePohdNOp5JO3wS9
XvkBJ6Wua7GBAiAdx+EKmdjVrwnzrQltTgnmSfGMXhKNYifK3uD83W3pcQ==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDMwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDQwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQUXDgcUVNT
9hovbZE5HL6rjOb7C55wEuWKThV/CcZ4rWrXx7VXHYdD/R3aDA7JSvYpm2sTok4i
sblDzhZM/GDNo4GJMIGGMB0GA1UdDgQWBBQox4F1NsZunlsduoGvzIgRSYfB3zBX
BgNVHSMEUDBOgBQApzZdtBdD3dLxouQpr/aDiVttd6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAyggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgAkiNhqFAZXSUWEDK91OZvQGdeZOtd6mC
+Wv3fGk3t28CIEKOwidkUTUaiPdZ4efmAr+CEeGzdq27ob2S+nqqHqgV
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDIwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDMwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQRDXDNIi1p
ereudhqwa2LslXgsxnB63Hu5y5lg+1WPruIYPzD/Ho0APveVdzFLVji19+bE4+tF
PYL1SpsN1WfWo4GJMIGGMB0GA1UdDgQWBBQApzZdtBdD3dLxouQpr/aDiVttdzBX
BgNVHSMEUDBOgBT5RCgQ0AlZTQbfFB2+6+w0XRvydaEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAxggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAOnd+7bAofkHVa4KFNjv3TCegw1lrhuM
8Of8wgvrTEGoAiEAsS8iKMpSfXH4D0egg4gLamE6akde965rDtySU+ve9lg=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDEwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDIwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQWHpv1i6lf

wvNPOP5ka6S0n55EvzoaYK6pbTXP6yMOW/4XZSPKx5Zoq4FMe0cKzGIIFL1rzj1V
2czYB+qvLhyio4GJMIGGMB0GA1UdDgQWBBT5RCgQ0AlZTQbfFB2+6+w0XRvydTBX
BgNVHSMEUDBOgBSh3uHkX5nj86yFEFwjscSWM40P+qEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAI7unGW/gr9tOc3i+dF5N815srgh+FrX
oj9Et74EcSpTAiBubv+vOH0DE0gmYI11HeAIgutWqqMIC72dZlwTF/Vi3g==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB3jCCAYWgAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDAwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQznn9zHHwL
GO8VR4W9V7vMlxCdoojzEOiX5Y6JtPtFOz866ueHY6zoN0/mJ6DnqnSXilJIUUeW
6eGfqmka7nxko4GRMIGOMB0GA1UdDgQWBBSh3uHkX5nj86yFEFwjscSWM40P+jBf
BgNVHSMEWDBWgBQlFYvU5WboI4fcdPoiQs8/fPHZraEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggkA/KCWhcqToHAw
DAYDVR0TBAUwAwEB/zAKBggqhkjOPQQDAgNHADBEAiBasbuinP+pJTU4oDCVD8zQ
1rJBDSOKIEyWu84/D6Hj6wIgVMPUoO01bPhzllAa/gW8Xk/daey09SBgN3AT9pWU
TDA=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIBpTCCAUugAwIBAgIJAPygloXKk6BwMAoGCCqGSM49BAMCMC8xCzAJBgNVBAYT
AlVLMREwDwYDVQQKDAhtYmVkIFRMUzENMAsGA1UEAwwEQ0EwMDAeFw0xNzA2MjIx
MTUwMzJaFw0yNzA2MjMxMTUwMzJaMC8xCzAJBgNVBAYTAlVLMREwDwYDVQQKDAht
YmVkIFRMUzENMAsGA1UEAwwEQ0EwMDBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IA
BFW41/qAwAPpy+Txdc7PKmzZsq9CPiujKU4vpF1ekXnGx2HP420QobwBVVWhkzRm
LwdboH2j65dcCKjQ7mv/dxKjUDBOMB0GA1UdDgQWBBQlFYvU5WboI4fcdPoiQs8/
fPHZrTAfBgNVHSMEGDAWgBQlFYvU5WboI4fcdPoiQs8/fPHZrTAMBgNVHRMEBTAD
AQH/MAoGCCqGSM49BAMCA0gAMEUCIQC7iRcVzwMyfVK5imirJ7MqJQ04euH4CLOt
IZ+SNfaERAIgSU0MWFDosVEIpg8YMqIHeF7Mg4ZyH6+fGazJgVLttUY=
-----END
CERTIFICATE-----
X509 Certificate information #1
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_SHA1_C
x509_cert_info:"data_files/server1.crt":"cert. version \: 3\nserial number \: 01\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nsubject name \: C=NL, O=PolarSSL, CN=PolarSSL Server 1\nissued on \: 2011-02-12 14\:44\:06\nexpires on \: 2021-02-12 14\:44\:06\nsigned using \: RSA with SHA1\nRSA key size \: 2048 bits\nbasic constraints \: CA=false\n"

X509 Certificate information #2
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_SHA1_C
x509_cert_info:"data_files/server2.crt":"cert. version \: 3\nserial number \: 02\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nsubject name \: C=NL, O=PolarSSL, CN=localhost\nissued on \: 2011-02-12 14\:44\:06\nexpires on \: 2021-02-12 14\:44\:06\nsigned using \: RSA with SHA1\nRSA key size \: 2048 bits\nbasic constraints \: CA=false\n"

X509 Certificate information

#3
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_SHA1_C
x509_cert_info:"data_files/test-ca.crt":"cert. version \: 3\nserial number \: 00\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nsubject name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nissued on \: 2011-02-12 14\:44\:00\nexpires on \: 2021-02-12 14\:44\:00\nsigned using \: RSA with SHA1\nRSA key size \: 2048 bits\nbasic constraints \: CA=true\n"

X509 Certificate information MD2 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509_cert_info:"data_files/cert_md2.crt":"cert. version \: 3\nserial number \: 09\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nsubject name \: C=NL, O=PolarSSL, CN=PolarSSL Cert MD2\nissued on \: 2009-07-12 10\:56\:59\nexpires on \: 2011-07-12 10\:56\:59\nsigned using \: RSA with MD2\nRSA key size \: 2048 bits\nbasic constraints \: CA=false\n"

X509 Certificate information MD4
Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_MD4_C
x509_cert_info:"data_files/cert_md4.crt":"cert. version \: 3\nserial number \: 05\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nsubject name \: C=NL, O=PolarSSL, CN=PolarSSL Cert MD4\nissued on \: 2011-02-12 14\:44\:07\nexpires on \: 2021-02-12 14\:44\:07\nsigned using \: RSA with MD4\nRSA key size \: 2048 bits\nbasic constraints \: CA=false\n"

X509 Certificate information MD5 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_MD5_C
x509_cert_info:"data_files/cert_md5.crt":"cert. version \: 3\nserial number \: 06\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nsubject name \: C=NL, O=PolarSSL, CN=PolarSSL Cert MD5\nissued on \: 2011-02-12 14\:44\:07\nexpires on \: 2021-02-12 14\:44\:07\nsigned using \: RSA with MD5\nRSA key size \: 2048 bits\nbasic constraints \: CA=false\n"

X509 Certificate information SHA1
Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_SHA1_C
x509_cert_info:"data_files/cert_sha1.crt":"cert. version \: 3\nserial number \: 07\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nsubject name \: C=NL, O=PolarSSL, CN=PolarSSL Cert SHA1\nissued on \: 2011-02-12 14\:44\:07\nexpires on \: 2021-02-12 14\:44\:07\nsigned using \: RSA with SHA1\nRSA key size \: 2048 bits\nbasic constraints \: CA=false\n"

X509 Certificate information SHA224 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_SHA256_C
x509_cert_info:"data_files/cert_sha224.crt":"cert. version \: 3\nserial number \: 08\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nsubject name \: C=NL, O=PolarSSL, CN=PolarSSL Cert SHA224\nissued on \: 2011-02-12 14\:44\:07\nexpires on \: 2021-02-12 14\:44\:07\nsigned using \: RSA with SHA-224\nRSA key size \: 2048 bits\nbasic constraints \: CA=false\n"

X509 Certificate
information SHA256 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_SHA256_C
x509_cert_info:"data_files/cert_sha256.crt":"cert. version \: 3\nserial number \: 09\nissuer name \: C=NL,

O=PolarSSL, CN=PolarSSL Test CA\nsubject name \: C=NL, O=PolarSSL, CN=PolarSSL Cert SHA256\nissued on \: 2011-02-12 14\:44\:07\nexpires on \: 2021-02-12 14\:44\:07\nsigned using \: RSA with SHA-256\nRSA key size \: 2048 bits\nbasic constraints \: CA=false\n"

X509 Certificate information SHA384 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_SHA512_C
x509_cert_info:"data_files/cert_sha384.crt":"cert. version \: 3\nserial number \: 0A\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nsubject name \: C=NL, O=PolarSSL, CN=PolarSSL Cert SHA384\nissued on \: 2011-02-12 14\:44\:07\nexpires on \: 2021-02-12 14\:44\:07\nsigned using \: RSA with SHA-384\nRSA key size \: 2048 bits\nbasic constraints
\: CA=false\n"

X509 Certificate information SHA512 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_SHA512_C
x509_cert_info:"data_files/cert_sha512.crt":"cert. version \: 3\nserial number \: 0B\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nsubject name \: C=NL, O=PolarSSL, CN=PolarSSL Cert SHA512\nissued on \: 2011-02-12 14\:44\:07\nexpires on \: 2021-02-12 14\:44\:07\nsigned using \: RSA with SHA-512\nRSA key size \: 2048 bits\nbasic constraints \: CA=false\n"

X509 Certificate information RSA-PSS, SHA1 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_X509_RSASSA_PSS_SUPPORT:MBEDTLS_SHA1_C
x509_cert_info:"data_files/server9.crt":"cert. version \: 3\nserial number \: 16\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nsubject name \: C=NL, O=PolarSSL, CN=localhost\nissued on \: 2014-01-20 13\:38\:16\nexpires on \: 2024-01-18 13\:38\:16\nsigned using \: RSASSA-PSS (SHA1, MGF1-SHA1,
0xEA)\nRSA key size \: 1024 bits\nbasic constraints \: CA=false\n"

X509 Certificate information RSA-PSS, SHA224 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_X509_RSASSA_PSS_SUPPORT:MBEDTLS_SHA256_C
x509_cert_info:"data_files/server9-sha224.crt":"cert. version \: 3\nserial number \: 17\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nsubject name \: C=NL, O=PolarSSL, CN=localhost\nissued on \: 2014-01-20 13\:57\:36\nexpires on \: 2024-01-18 13\:57\:36\nsigned using \: RSASSA-PSS (SHA224, MGF1-SHA224, 0xE2)\nRSA key size \: 1024 bits\nbasic constraints \: CA=false\n"

X509 Certificate information RSA-PSS, SHA256 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_X509_RSASSA_PSS_SUPPORT:MBEDTLS_SHA256_C
x509_cert_info:"data_files/server9-sha256.crt":"cert. version \: 3\nserial number \: 18\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nsubject name \: C=NL, O=PolarSSL, CN=localhost\nissued on \: 2014-01-20
13\:57\:45\nexpires on \: 2024-01-18 13\:57\:45\nsigned using \: RSASSA-PSS (SHA256, MGF1-SHA256, 0xDE)\nRSA key size \: 1024 bits\nbasic constraints \: CA=false\n"

X509 Certificate information RSA-PSS, SHA384 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_X509_RSASSA_PSS_SUPPORT:MBEDTLS_SHA512_C
x509_cert_info:"data_files/server9-sha384.crt":"cert. version \: 3\nserial number \: 19\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nsubject name \: C=NL, O=PolarSSL, CN=localhost\nissued on \: 2014-01-20 13\:57\:58\nexpires on \: 2024-01-18 13\:57\:58\nsigned using \: RSASSA-PSS (SHA384, MGF1-SHA384, 0xCE)\nRSA key size \: 1024 bits\nbasic constraints \: CA=false\n"

X509 Certificate information RSA-PSS, SHA512 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_X509_RSASSA_PSS_SUPPORT:MBEDTLS_SHA512_C
x509_cert_info:"data_files/server9-sha512.crt":"cert. version \: 3\nserial number \: 1A\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nsubject name \: C=NL, O=PolarSSL, CN=localhost\nissued on \: 2014-01-20 13\:58\:12\nexpires on \: 2024-01-18 13\:58\:12\nsigned using \: RSASSA-PSS (SHA512, MGF1-SHA512, 0xBE)\nRSA key size \: 1024 bits\nbasic constraints \: CA=false\n"

X509 Certificate information EC, SHA1 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA1_C
x509_cert_info:"data_files/server5-sha1.crt":"cert. version \: 3\nserial number \: 12\nissuer name \: C=NL, O=PolarSSL, CN=Polarssl Test EC CA\nsubject name \: C=NL, O=PolarSSL, CN=localhost\nissued on \: 2013-09-24 16\:21\:27\nexpires on \: 2023-09-22 16\:21\:27\nsigned using \: ECDSA with SHA1\nEC key size \: 256 bits\nbasic constraints \: CA=false\n"

X509 Certificate information EC, SHA224 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA256_C
x509_cert_info:"data_files/server5-sha224.crt":"cert.
version \: 3\nserial number \: 13\nissuer name \: C=NL, O=PolarSSL, CN=Polarssl Test EC CA\nsubject name \: C=NL, O=PolarSSL, CN=localhost\nissued on \: 2013-09-24 16\:21\:27\nexpires on \: 2023-09-22 16\:21\:27\nsigned using \: ECDSA with SHA224\nEC key size \: 256 bits\nbasic constraints \: CA=false\n"

X509 Certificate information EC, SHA256 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA256_C
x509_cert_info:"data_files/server5.crt":"cert. version \: 3\nserial number \: 09\nissuer name \: C=NL, O=PolarSSL, CN=Polarssl Test EC CA\nsubject name \: C=NL, O=PolarSSL, CN=localhost\nissued on \: 2013-09-24 15\:52\:04\nexpires on \: 2023-09-22 15\:52\:04\nsigned using \: ECDSA with SHA256\nEC key size \: 256 bits\nbasic constraints \: CA=false\n"

X509 Certificate information EC, SHA384 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA512_C
x509_cert_info:"data_files/server5-sha384.crt":"cert.
version \: 3\nserial number \: 14\nissuer name \: C=NL, O=PolarSSL, CN=Polarssl Test EC CA\nsubject name \: C=NL, O=PolarSSL, CN=localhost\nissued on \: 2013-09-24 16\:21\:27\nexpires on \: 2023-09-22 16\:21\:27\nsigned using \: ECDSA with SHA384\nEC key size \: 256 bits\nbasic constraints \: CA=false\n"

X509 Certificate information EC, SHA512 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA512_C
x509_cert_info:"data_files/server5-sha512.crt":"cert. version \: 3\nserial number \: 15\nissuer name \: C=NL, O=PolarSSL, CN=Polarssl Test EC CA\nsubject name \: C=NL, O=PolarSSL, CN=localhost\nissued on \: 2013-09-24 16\:21\:27\nexpires on \: 2023-09-22 16\:21\:27\nsigned using \: ECDSA with

SHA512\nEC key size \: 256 bits\nbasic
constraints \: CA=false\n"

X509 Certificate information, NS Cert Type
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_SHA1_C
x509_cert_info:"data_files/server1.cert_type.crt":"cert. version \: 3\nserial number \: 01\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nsubject name \: C=NL, O=PolarSSL, CN=PolarSSL Server 1\nissued on \: 2011-02-12 14\:44\:06\nexpires on \: 2021-02-12 14\:44\:06\nsigned using \: RSA with SHA1\nRSA key size \: 2048 bits\nbasic constraints \: CA=false\ncert. type \: SSL Server\n"

X509 Certificate information, Key Usage
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_SHA1_C
x509_cert_info:"data_files/server1.key_usage.crt":"cert. version \: 3\nserial number \: 01\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nsubject name \: C=NL, O=PolarSSL, CN=PolarSSL Server 1\nissued on \: 2011-02-12 14\:44\:06\nexpires on \: 2021-02-12 14\:44\:06\nsigned using \: RSA with SHA1\nRSA key size \: 2048 bits\nbasic constraints \: CA=false\nkey usage \: Digital Signature, Non Repudiation, Key Encipherment\n"

X509 Certificate information, Key Usage with decipherOnly
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_SHA1_C
x509_cert_info:"data_files/keyUsage.decipherOnly.crt":"cert. version \: 3\nserial number \: 9B\:13\:CE\:4C\:A5\:6F\:DE\:52\nissuer name \: C=GB, L=Cambridge, O=Default Company Ltd\nsubject name \: C=GB, L=Cambridge, O=Default Company Ltd\nissued on \: 2015-05-12 10\:36\:55\nexpires on \: 2018-05-11 10\:36\:55\nsigned using \: RSA with SHA1\nRSA key size \: 1024 bits\nbasic constraints \: CA=false\nkey usage \: Digital Signature, Non Repudiation, Key Encipherment, Decipher Only\n"

X509 Certificate information, Subject Alt Name
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_SHA1_C
x509_cert_info:"data_files/cert_example_multi.crt":"cert. version \:
3\nserial number \: 11\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nsubject name \: C=NL, O=PolarSSL, CN=www.example.com\nissued on \: 2012-05-10 13\:23\:41\nexpires on \: 2022-05-11 13\:23\:41\nsigned using \: RSA with SHA1\nRSA key size \: 2048 bits\nbasic constraints \: CA=false\nsubject alt name \: example.com, example.net, *.example.org\n"

X509 Certificate information, Subject Alt Name + Key Usage
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_SHA1_C
x509_cert_info:"data_files/cert_example_multi_nocn.crt":"cert. version \: 3\nserial number \: F7\:C6\:7F\:F8\:E9\:A9\:63\:F9\nissuer name \: C=NL\nsubject name \: C=NL\nissued on \: 2014-01-22 10\:04\:33\nexpires on \: 2024-01-22 10\:04\:33\nsigned using \: RSA with SHA1\nRSA key size \: 1024 bits\nbasic constraints \: CA=false\nsubject alt name \: www.shotokan-braunschweig.de, www.massimo-abate.eu\nkey usage \: Digital Signature,
Non Repudiation, Key Encipherment\n"

X509 Certificate information, Key Usage + Extended Key Usage
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_SHA256_C
x509_cert_info:"data_files/server1.ext_ku.crt":"cert. version \: 3\nserial number \: 21\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nsubject name \: C=NL, O=PolarSSL, CN=PolarSSL Server 1\nissued on \: 2014-04-01 14\:44\:43\nexpires on \: 2024-03-29 14\:44\:43\nsigned using \: RSA with

SHA-256\nRSA key size \: 2048 bits\nbasic constraints \: CA=false\nkey usage \: Digital Signature, Non Repudiation, Key Encipherment\next key usage \: TLS Web Server Authentication\n"

X509 Certificate information RSA signed by EC
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_SHA256_C:MBEDTLS_ECDSA_C
x509_cert_info:"data_files/server4.crt":"cert. version \: 3\nserial number \: 08\nissuer name \: C=NL, O=PolarSSL, CN=Polarssl Test EC CA\nsubject name
\: C=NL, O=PolarSSL, CN=localhost\nissued on \: 2013-09-24 15\:52\:04\nexpires on \: 2023-09-22 15\:52\:04\nsigned using \: ECDSA with SHA256\nRSA key size \: 2048 bits\nbasic constraints \: CA=false\n"

X509 Certificate information EC signed by RSA
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP192R1_ENABLED:MBEDTLS_SHA1_C
x509_cert_info:"data_files/server3.crt":"cert. version \: 3\nserial number \: 0D\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nsubject name \: C=NL, O=PolarSSL, CN=localhost\nissued on \: 2013-08-09 09\:17\:03\nexpires on \: 2023-08-07 09\:17\:03\nsigned using \: RSA with SHA1\nEC key size \: 192 bits\nbasic constraints \: CA=false\n"

X509 Certificate information Bitstring in subject name
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_SHA1_C
x509_cert_info:"data_files/bitstring-in-dn.pem":"cert. version \: 3\nserial number \: 02\nissuer name \: CN=Test
CA 01, ST=Ecnivorp, C=XX, emailAddress=tca@example.com, O=Test CA Authority\nsubject name \: C=XX, O=tca, ST=Ecnivorp, OU=TCA, CN=Client, emailAddress=client@example.com, serialNumber=7101012255, uniqueIdentifier=?7101012255\nissued on \: 2015-03-11 12\:06\:51\nexpires on \: 2025-03-08 12\:06\:51\nsigned using \: RSA with SHA1\nRSA key size \: 2048 bits\nbasic constraints \: CA=false\nsubject alt name \: \next key usage \: TLS Web Client Authentication\n"

X509 certificate v1 with extension
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_X509_ALLOW_EXTENSIONS_NON_V3:MBEDTLS_SHA1_C
x509_cert_info:"data_files/cert_v1_with_ext.crt":"cert. version \: 1\nserial number \: BD\:ED\:44\:C7\:D2\:3E\:C2\:A4\nissuer name \: C=XX, ST=XX, L=XX, O=XX, OU=XX, emailAddress=admin@identity-check.org, CN=identity-check.org\nsubject name \: C=XX, ST=XX, L=XX, O=XX, OU=XX, emailAddress=admin@identity-check.org, CN=identity-check.org\nissued on \: 2013-07-04 16\:17\:02\nexpires on \: 2014-07-04 16\:17\:02\nsigned using \: RSA with SHA1\nRSA key size \: 2048 bits\nsubject alt name \: identity-check.org, www.identity-check.org\n"

X509 CRL information #1
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C
mbedtls_x509_crl_info:"data_files/crl_expired.pem":"CRL version \: 1\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nthis update \: 2011-02-20 10\:24\:19\nnext update \: 2011-02-20 11\:24\:19\nRevoked certificates\:\nserial number\: 01 revocation date\: 2011-02-12 14\:44\:07\nserial number\: 03 revocation date\: 2011-02-12 14\:44\:07\nsigned using \: RSA with SHA1\n"

X509 CRL Information MD2 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_MD2_C

mbedtls_x509_crl_info:"data_files/crl_md2.pem":"CRL version \: 1\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nthis update \: 2009-07-19 19\:56\:37\nnext update \: 2009-09-17 19\:56\:37\nRevoked certificates\:\nserial number\: 01 revocation
date\: 2009-02-09 21\:12\:36\nserial number\: 03 revocation date\: 2009-02-09 21\:12\:36\nsigned using \: RSA with MD2\n"

X509 CRL Information MD4 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_MD4_C
mbedtls_x509_crl_info:"data_files/crl_md4.pem":"CRL version \: 1\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nthis update \: 2011-02-12 14\:44\:07\nnext update \: 2011-04-13 14\:44\:07\nRevoked certificates\:\nserial number\: 01 revocation date\: 2011-02-12 14\:44\:07\nserial number\: 03 revocation date\: 2011-02-12 14\:44\:07\nsigned using \: RSA with MD4\n"

X509 CRL Information MD5 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_MD5_C
mbedtls_x509_crl_info:"data_files/crl_md5.pem":"CRL version \: 1\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nthis update \: 2011-02-12 14\:44\:07\nnext update \: 2011-04-13 14\:44\:07\nRevoked certificates\:\nserial number\: 01 revocation date\: 2011-02-12 14\:44\:07\nserial number\: 03 revocation date\: 2011-02-12
14\:44\:07\nsigned using \: RSA with MD5\n"

X509 CRL Information SHA1 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C
mbedtls_x509_crl_info:"data_files/crl_sha1.pem":"CRL version \: 1\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nthis update \: 2011-02-12 14\:44\:07\nnext update \: 2011-04-13 14\:44\:07\nRevoked certificates\:\nserial number\: 01 revocation date\: 2011-02-12 14\:44\:07\nserial number\: 03 revocation date\: 2011-02-12 14\:44\:07\nsigned using \: RSA with SHA1\n"

X509 CRL Information SHA224 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA256_C
mbedtls_x509_crl_info:"data_files/crl_sha224.pem":"CRL version \: 1\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nthis update \: 2011-02-12 14\:44\:07\nnext update \: 2011-04-13 14\:44\:07\nRevoked certificates\:\nserial number\: 01 revocation date\: 2011-02-12 14\:44\:07\nserial number\: 03 revocation date\: 2011-02-12 14\:44\:07\nsigned using \: RSA with SHA-224\n"

X509 CRL Information
SHA256 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA256_C
mbedtls_x509_crl_info:"data_files/crl_sha256.pem":"CRL version \: 1\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nthis update \: 2011-02-12 14\:44\:07\nnext update \: 2011-04-13 14\:44\:07\nRevoked certificates\:\nserial number\: 01 revocation date\: 2011-02-12 14\:44\:07\nserial number\: 03 revocation date\: 2011-02-12 14\:44\:07\nsigned using \: RSA with SHA-256\n"

X509 CRL Information SHA384 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA512_C
mbedtls_x509_crl_info:"data_files/crl_sha384.pem":"CRL version \: 1\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nthis update \: 2011-02-12 14\:44\:07\nnext update \: 2011-04-13 14\:44\:07\nRevoked certificates\:\nserial number\: 01 revocation date\: 2011-02-12 14\:44\:07\nserial number\: 03 revocation date\: 2011-

02-12 14\:44\:07\nsigned using \: RSA with SHA-384\n"

X509 CRL Information SHA512 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA512_C
mbedtls_x509_crl_info:"data_files/crl_sha512.pem":"CRL
 version \: 1\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nthis update \: 2011-02-12 14\:44\:07\nnext update \: 2011-04-13 14\:44\:07\nRevoked certificates\:\nserial number\: 01 revocation date\: 2011-02-12 14\:44\:07\nserial number\: 03 revocation date\: 2011-02-12 14\:44\:07\nsigned using \: RSA with SHA-512\n"

X509 CRL information RSA-PSS, SHA1 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_X509_RSASSA_PSS_SUPPORT:MBEDTLS_SHA1_C
mbedtls_x509_crl_info:"data_files/crl-rsa-pss-sha1.pem":"CRL version \: 2\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nthis update \: 2014-01-20 13\:46\:35\nnext update \: 2024-01-18 13\:46\:35\nRevoked certificates\:\nserial number\: 0A revocation date\: 2013-09-24 16\:28\:38\nserial number\: 16 revocation date\: 2014-01-20 13\:43\:05\nsigned using \: RSASSA-PSS (SHA1, MGF1-SHA1, 0xEA)\n"

X509 CRL information RSA-PSS, SHA224 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_X509_RSASSA_PSS_SUPPORT:MBEDTLS_SHA256_C
mbedtls_x509_crl_info:"data_files/crl-rsa-pss-sha224.pem":"CRL
 version \: 2\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nthis update \: 2014-01-20 13\:56\:06\nnext update \: 2024-01-18 13\:56\:06\nRevoked certificates\:\nserial number\: 0A revocation date\: 2013-09-24 16\:28\:38\nserial number\: 16 revocation date\: 2014-01-20 13\:43\:05\nsigned using \: RSASSA-PSS (SHA224, MGF1-SHA224, 0xE2)\n"

X509 CRL information RSA-PSS, SHA256 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_X509_RSASSA_PSS_SUPPORT:MBEDTLS_SHA256_C
mbedtls_x509_crl_info:"data_files/crl-rsa-pss-sha256.pem":"CRL version \: 2\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nthis update \: 2014-01-20 13\:56\:16\nnext update \: 2024-01-18 13\:56\:16\nRevoked certificates\:\nserial number\: 0A revocation date\: 2013-09-24 16\:28\:38\nserial number\: 16 revocation date\: 2014-01-20 13\:43\:05\nsigned using \: RSASSA-PSS (SHA256, MGF1-SHA256, 0xDE)\n"

X509 CRL information RSA-PSS, SHA384 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_X509_RSASSA_PSS_SUPPORT:MBEDTLS_SHA512_C
mbedtls_x509_crl_info:"data_files/crl-rsa-pss-sha384.pem":"CRL version \: 2\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nthis update \: 2014-01-20 13\:56\:28\nnext update \: 2024-01-18 13\:56\:28\nRevoked certificates\:\nserial number\: 0A revocation date\: 2013-09-24 16\:28\:38\nserial number\: 16 revocation date\: 2014-01-20 13\:43\:05\nsigned using \: RSASSA-PSS (SHA384, MGF1-SHA384, 0xCE)\n"

X509 CRL information RSA-PSS, SHA512 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_X509_RSASSA_PSS_SUPPORT:MBEDTLS_SHA512_C
mbedtls_x509_crl_info:"data_files/crl-rsa-pss-sha512.pem":"CRL version \: 2\nissuer name \: C=NL, O=PolarSSL, CN=PolarSSL Test CA\nthis update \: 2014-01-20 13\:56\:38\nnext update \: 2024-01-18 13\:56\:38\nRevoked certificates\:\nserial number\: 0A revocation date\: 2013-09-24 16\:28\:38\nserial number\: 16 revocation date\: 2014-01-20 13\:43\:05\nsigned using \: RSASSA-PSS (SHA512, MGF1-SHA512, 0xBE)\n"

X509 CRL Information EC, SHA1 Digest

depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C
mbedtls_x509_crl_info:"data_files/crl-ec-sha1.pem":"CRL version \: 2\nissuer name \: C=NL, O=PolarSSL, CN=Polarssl Test EC CA\nthis update \: 2013-09-24 16\:31\:08\nnext update \: 2023-09-22 16\:31\:08\nRevoked certificates\:\nserial number\: 0A revocation date\: 2013-09-24 16\:28\:38\nsigned using \: ECDSA with SHA1\n"

X509 CRL Information EC, SHA224 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA256_C
mbedtls_x509_crl_info:"data_files/crl-ec-sha224.pem":"CRL version \: 2\nissuer name \: C=NL, O=PolarSSL, CN=Polarssl Test EC CA\nthis update \: 2013-09-24 16\:31\:08\nnext update \: 2023-09-22 16\:31\:08\nRevoked certificates\:\nserial number\: 0A revocation date\: 2013-09-24 16\:28\:38\nsigned using \: ECDSA with SHA224\n"

X509 CRL Information EC, SHA256 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA256_C
mbedtls_x509_crl_info:"data_files/crl-ec-sha256.pem":"CRL
version \: 2\nissuer name \: C=NL, O=PolarSSL, CN=Polarssl Test EC CA\nthis update \: 2013-09-24 16\:31\:08\nnext update \: 2023-09-22 16\:31\:08\nRevoked certificates\:\nserial number\: 0A revocation date\: 2013-09-24 16\:28\:38\nsigned using \: ECDSA with SHA256\n"

X509 CRL Information EC, SHA384 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA512_C
mbedtls_x509_crl_info:"data_files/crl-ec-sha384.pem":"CRL version \: 2\nissuer name \: C=NL, O=PolarSSL, CN=Polarssl Test EC CA\nthis update \: 2013-09-24 16\:31\:08\nnext update \: 2023-09-22 16\:31\:08\nRevoked certificates\:\nserial number\: 0A revocation date\: 2013-09-24 16\:28\:38\nsigned using \: ECDSA with SHA384\n"

X509 CRL Information EC, SHA512 Digest
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA512_C
mbedtls_x509_crl_info:"data_files/crl-ec-sha512.pem":"CRL version \: 2\nissuer name \: C=NL, O=PolarSSL, CN=Polarssl Test EC
CA\nthis update \: 2013-09-24 16\:31\:08\nnext update \: 2023-09-22 16\:31\:08\nRevoked certificates\:\nserial number\: 0A revocation date\: 2013-09-24 16\:28\:38\nsigned using \: ECDSA with SHA512\n"

X509 CRL Malformed Input (trailing spaces at end of file)
depends_on:MBEDTLS_PEM_PARSE_C
mbedtls_x509_crl_parse:"data_files/crl-malformed-trailing-spaces.pem":MBEDTLS_ERR_PEM_NO_HEADER_FOOTER_PRESENT

X509 CSR Information RSA with MD4
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_MD4_C
mbedtls_x509_csr_info:"data_files/server1.req.md4":"CSR version \: 1\nsubject name \: C=NL, O=PolarSSL, CN=PolarSSL Server 1\nsigned using \: RSA with MD4\nRSA key size \: 2048 bits\n"

X509 CSR Information RSA with MD5
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_MD5_C
mbedtls_x509_csr_info:"data_files/server1.req.md5":"CSR version \: 1\nsubject name \: C=NL, O=PolarSSL, CN=PolarSSL Server 1\nsigned using \: RSA with MD5\nRSA key size \: 2048 bits\n"

X509 CSR Information RSA with SHA1
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C

mbedtls_x509_csr_info:"data_files/server1.req.sha1":"CSR
version \: 1\nsubject name \: C=NL, O=PolarSSL, CN=PolarSSL Server 1\nsigned using \: RSA with SHA1\nRSA key size \: 2048 bits\n"

X509 CSR Information RSA with SHA224
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA256_C
mbedtls_x509_csr_info:"data_files/server1.req.sha224":"CSR version \: 1\nsubject name \: C=NL, O=PolarSSL, CN=PolarSSL Server 1\nsigned using \: RSA with SHA-224\nRSA key size \: 2048 bits\n"

X509 CSR Information RSA with SHA256
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA256_C
mbedtls_x509_csr_info:"data_files/server1.req.sha256":"CSR version \: 1\nsubject name \: C=NL, O=PolarSSL, CN=PolarSSL Server 1\nsigned using \: RSA with SHA-256\nRSA key size \: 2048 bits\n"

X509 CSR Information RSA with SHA384
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA512_C
mbedtls_x509_csr_info:"data_files/server1.req.sha384":"CSR version \: 1\nsubject name \: C=NL, O=PolarSSL, CN=PolarSSL Server
1\nsigned using \: RSA with SHA-384\nRSA key size \: 2048 bits\n"

X509 CSR Information RSA with SHA512
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA512_C
mbedtls_x509_csr_info:"data_files/server1.req.sha512":"CSR version \: 1\nsubject name \: C=NL, O=PolarSSL, CN=PolarSSL Server 1\nsigned using \: RSA with SHA-512\nRSA key size \: 2048 bits\n"

X509 CSR Information EC with SHA1
depends_on:MBEDTLS_ECP_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA1_C
mbedtls_x509_csr_info:"data_files/server5.req.sha1":"CSR version \: 1\nsubject name \: C=NL, O=PolarSSL, CN=localhost\nsigned using \: ECDSA with SHA1\nEC key size \: 256 bits\n"

X509 CSR Information EC with SHA224
depends_on:MBEDTLS_ECP_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA256_C
mbedtls_x509_csr_info:"data_files/server5.req.sha224":"CSR version \: 1\nsubject name \: C=NL, O=PolarSSL, CN=localhost\nsigned using \: ECDSA with SHA224\nEC key size \: 256 bits\n"

X509 CSR Information
EC with SHA256
depends_on:MBEDTLS_ECP_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA256_C
mbedtls_x509_csr_info:"data_files/server5.req.sha256":"CSR version \: 1\nsubject name \: C=NL, O=PolarSSL, CN=localhost\nsigned using \: ECDSA with SHA256\nEC key size \: 256 bits\n"

X509 CSR Information EC with SHA384
depends_on:MBEDTLS_ECP_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA512_C
mbedtls_x509_csr_info:"data_files/server5.req.sha384":"CSR version \: 1\nsubject name \: C=NL, O=PolarSSL,

CN=localhost\nsigned using \: ECDSA with SHA384\nEC key size \: 256 bits\n"

X509 CSR Information EC with SHA512
depends_on:MBEDTLS_ECP_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA512_C
mbedtls_x509_csr_info:"data_files/server5.req.sha512":"CSR version \: 1\nsubject name \: C=NL, O=PolarSSL, CN=localhost\nsigned using \: ECDSA with SHA512\nEC key size \: 256 bits\n"

X509 CSR Information RSA-PSS with SHA1
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_X509_RSASSA_PSS_SUPPORT:MBEDTLS_SHA1_C
mbedtls_x509_csr_info:"data_files/server9.req.sha1":"CSR
 version \: 1\nsubject name \: C=NL, O=PolarSSL, CN=localhost\nsigned using \: RSASSA-PSS (SHA1, MGF1-SHA1, 0x6A)\nRSA key size \: 1024 bits\n"

X509 CSR Information RSA-PSS with SHA224
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_X509_RSASSA_PSS_SUPPORT:MBEDTLS_SHA256_C
mbedtls_x509_csr_info:"data_files/server9.req.sha224":"CSR version \: 1\nsubject name \: C=NL, O=PolarSSL, CN=localhost\nsigned using \: RSASSA-PSS (SHA224, MGF1-SHA224, 0x62)\nRSA key size \: 1024 bits\n"

X509 CSR Information RSA-PSS with SHA256
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_X509_RSASSA_PSS_SUPPORT:MBEDTLS_SHA256_C
mbedtls_x509_csr_info:"data_files/server9.req.sha256":"CSR version \: 1\nsubject name \: C=NL, O=PolarSSL, CN=localhost\nsigned using \: RSASSA-PSS (SHA256, MGF1-SHA256, 0x5E)\nRSA key size \: 1024 bits\n"

X509 CSR Information RSA-PSS with SHA384
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_X509_RSASSA_PSS_SUPPORT:MBEDTLS_SHA512_C
mbedtls_x509_csr_info:"data_files/server9.req.sha384":"CSR
 version \: 1\nsubject name \: C=NL, O=PolarSSL, CN=localhost\nsigned using \: RSASSA-PSS (SHA384, MGF1-SHA384, 0x4E)\nRSA key size \: 1024 bits\n"

X509 CSR Information RSA-PSS with SHA512
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_X509_RSASSA_PSS_SUPPORT:MBEDTLS_SHA512_C
mbedtls_x509_csr_info:"data_files/server9.req.sha512":"CSR version \: 1\nsubject name \: C=NL, O=PolarSSL, CN=localhost\nsigned using \: RSASSA-PSS (SHA512, MGF1-SHA512, 0x3E)\nRSA key size \: 1024 bits\n"

X509 Verify Information: empty
x509_verify_info:0:"":""

X509 Verify Information: one issue
x509_verify_info:MBEDTLS_X509_BADCERT_MISSING:"":"Certificate was missing\n"

X509 Verify Information: two issues
x509_verify_info:MBEDTLS_X509_BADCERT_EXPIRED | MBEDTLS_X509_BADCRL_EXPIRED:"":"The certificate validity has expired\nThe CRL is expired\n"

X509 Verify Information: two issues, one unknown
x509_verify_info:MBEDTLS_X509_BADCERT_OTHER

| 0x80000000:"":"Other reason (can be used by verify callback)\nUnknown reason (this should not happen)\n"

X509 Verify Information: empty, with prefix
x509_verify_info:0:" ! ":""

X509 Verify Information: one issue, with prefix
x509_verify_info:MBEDTLS_X509_BADCERT_MISSING:" ! ":" ! Certificate was missing\n"

X509 Verify Information: two issues, with prefix
x509_verify_info:MBEDTLS_X509_BADCERT_EXPIRED | MBEDTLS_X509_BADCRL_EXPIRED:" ! ":" ! The certificate validity has expired\n ! The CRL is expired\n"

X509 Get Distinguished Name #1
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_SHA1_C
mbedtls_x509_dn_gets:"data_files/server1.crt":"subject":"C=NL, O=PolarSSL, CN=PolarSSL Server 1"

X509 Get Distinguished Name #2
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_SHA1_C
mbedtls_x509_dn_gets:"data_files/server1.crt":"issuer":"C=NL, O=PolarSSL, CN=PolarSSL Test CA"

X509 Get Distinguished Name #3
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_SHA1_C
mbedtls_x509_dn_gets:"data_files/server2.crt":"subject":"C=NL,
O=PolarSSL, CN=localhost"

X509 Get Distinguished Name #4
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_SHA1_C
mbedtls_x509_dn_gets:"data_files/server2.crt":"issuer":"C=NL, O=PolarSSL, CN=PolarSSL Test CA"

X509 Time Expired #1
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_HAVE_TIME_DATE:MBEDTLS_SHA1_C
mbedtls_x509_time_is_past:"data_files/server1.crt":"valid_from":1

X509 Time Expired #2
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_HAVE_TIME_DATE:MBEDTLS_SHA1_C
mbedtls_x509_time_is_past:"data_files/server1.crt":"valid_to":0

X509 Time Expired #3
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_HAVE_TIME_DATE:MBEDTLS_SHA1_C
mbedtls_x509_time_is_past:"data_files/server2.crt":"valid_from":1

X509 Time Expired #4
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_HAVE_TIME_DATE:MBEDTLS_SHA1_C
mbedtls_x509_time_is_past:"data_files/server2.crt":"valid_to":0

X509 Time
Expired #5
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_HAVE_TIME_DATE:MBEDTLS_SHA1_C
mbedtls_x509_time_is_past:"data_files/test-ca.crt":"valid_from":1

X509 Time Expired #6
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_HAVE_TIME_DATE:MBEDTLS_SHA1_C
mbedtls_x509_time_is_past:"data_files/test-ca.crt":"valid_to":0

X509 Time Future #1
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_HAVE_TIME_DATE:MBEDTLS_SHA256_C
mbedtls_x509_time_is_future:"data_files/server5.crt":"valid_from":0

X509 Time Future #2
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_HAVE_TIME_DATE:MBEDTLS_SHA256_C
mbedtls_x509_time_is_future:"data_files/server5.crt":"valid_to":1

X509 Time Future #3
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_HAVE_TIME_DATE:MBEDTLS_SHA256_C
mbedtls_x509_time_is_future:"data_files/server5-future.crt":"valid_from":1

X509 Time Future #4
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_HAVE_TIME_DATE:MBEDTLS_SHA256_C
mbedtls_x509_time_is_future:"data_files/server5-future.crt":"valid_to":1

X509
Time Future #5
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_HAVE_TIME_DATE:MBEDTLS_SHA256_C
mbedtls_x509_time_is_future:"data_files/test-ca2.crt":"valid_from":0

X509 Time Future #6
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_HAVE_TIME_DATE:MBEDTLS_SHA256_C
mbedtls_x509_time_is_future:"data_files/test-ca2.crt":"valid_to":1

X509 Certificate verification #1 (Revoked Cert, Expired CRL, no CN)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_verify:"data_files/server1.crt":"data_files/test-ca.crt":"data_files/crl_expired.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_REVOKED | MBEDTLS_X509_BADCRL_EXPIRED:"compat":"NULL"

X509 Certificate verification #1a (Revoked Cert, Future CRL, no
CN)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA256_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA1_C
x509_verify:"data_files/server6.crt":"data_files/test-ca2.crt":"data_files/crl-future.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_REVOKED | MBEDTLS_X509_BADCRL_FUTURE:"compat":"NULL"

X509 Certificate verification #2 (Revoked Cert, Expired CRL)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_verify:"data_files/server1.crt":"data_files/test-ca.crt":"data_files/crl_expired.pem":"PolarSSL Server 1":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_REVOKED | MBEDTLS_X509_BADCRL_EXPIRED:"compat":"NULL"

X509 Certificate verification #2a (Revoked Cert, Future CRL)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA256_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA1_C
x509_verify:"data_files/server6.crt":"data_files/test-ca2.crt":"data_files/crl-future.pem":"localhost":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_REVOKED
| MBEDTLS_X509_BADCRL_FUTURE:"compat":"NULL"

X509 Certificate verification #3 (Revoked Cert, Future CRL, CN Mismatch)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_verify:"data_files/server1.crt":"data_files/test-ca.crt":"data_files/crl_expired.pem":"PolarSSL Wrong CN":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_REVOKED | MBEDTLS_X509_BADCRL_EXPIRED | MBEDTLS_X509_BADCERT_CN_MISMATCH:"compat":"NULL"

X509 Certificate verification #3a (Revoked Cert, Expired CRL, CN Mismatch)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA256_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA1_C
x509_verify:"data_files/server6.crt":"data_files/test-ca2.crt":"data_files/crl-future.pem":"Wrong CN":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_REVOKED | MBEDTLS_X509_BADCRL_FUTURE | MBEDTLS_X509_BADCERT_CN_MISMATCH:"compat":"NULL"

X509
Certificate verification #4 (Valid Cert, Expired CRL)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_verify:"data_files/server2.crt":"data_files/test-ca.crt":"data_files/crl_expired.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCRL_EXPIRED:"compat":"NULL"

X509 Certificate verification #4a (Revoked Cert, Future CRL)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA256_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA1_C
x509_verify:"data_files/server5.crt":"data_files/test-ca2.crt":"data_files/crl-future.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCRL_FUTURE:

"compat":"NULL"

X509 Certificate verification #5 (Revoked Cert)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_verify:"data_files/server1.crt":"data_files/test-
ca.crt":"data_files/crl.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BAD
CERT_REVOKED:"compat":"NULL"

X509
Certificate verification #6 (Revoked Cert)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_verify:"data_files/server1.crt":"data_files/test-ca.crt":"data_files/crl.pem":"PolarSSL Server
1":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_REVOKED:"compat":"NU
LL"

X509 Certificate verification #7 (Revoked Cert, CN Mismatch)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_verify:"data_files/server1.crt":"data_files/test-ca.crt":"data_files/crl.pem":"PolarSSL Wrong
CN":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_REVOKED |
MBEDTLS_X509_BADCERT_CN_MISMATCH:"compat":"NULL"

X509 Certificate verification #8 (Valid Cert)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA256_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SE
CP256R1_ENABLED:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA1_C
x509_verify:"data_files/server5.crt":"data_files/test-ca2.crt":"data_files/crl-ec-
sha1.pem":"NULL":0:0:"compat":"NULL"

X509 Certificate
verification #8a (Expired Cert)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA256_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SE
CP256R1_ENABLED:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA1_C
x509_verify:"data_files/server5-expired.crt":"data_files/test-ca2.crt":"data_files/crl-ec-
sha1.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_EXPIRE
D:"compat":"NULL"

X509 Certificate verification #8b (Future Cert)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA256_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SE
CP256R1_ENABLED:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA1_C
x509_verify:"data_files/server5-future.crt":"data_files/test-ca2.crt":"data_files/crl-ec-
sha1.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_FUTURE
:"compat":"NULL"

X509 Certificate verification #9 (Not trusted Cert)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_verify:"data_files/server2.crt":"data_files/server1.crt":"data_files/crl.pem":"NULL":MBEDTLS_ERR_X509_
CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_NOT_TRUSTED:"compat":"NULL"

X509

Certificate verification #10 (Not trusted Cert, Expired CRL)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15:MBEDTLS_SHA1_C
x509_verify:"data_files/server2.crt":"data_files/server1.crt":"data_files/crl_expired.pem":"NULL":MBEDTLS_ER
R_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_NOT_TRUSTED:"compat":"NULL"

X509 Certificate verification #12 (Valid Cert MD4 Digest)
depends_on:MBEDTLS_MD4_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBED
TLS_PKCS1_V15
x509_verify:"data_files/cert_md4.crt":"data_files/test-
ca.crt":"data_files/crl.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BAD
CERT_BAD_MD:"compat":"NULL"

X509 Certificate verification #13 (Valid Cert MD5 Digest)
depends_on:MBEDTLS_MD5_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBED
TLS_PKCS1_V15
x509_verify:"data_files/cert_md5.crt":"data_files/test-
ca.crt":"data_files/crl.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BAD
CERT_BAD_MD:"compat":"NULL"

X509
Certificate verification #14 (Valid Cert SHA1 Digest explicitly allowed in profile)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBE
DTLS_PKCS1_V15
x509_verify:"data_files/cert_sha1.crt":"data_files/test-ca.crt":"data_files/crl.pem":"NULL":0:0:"compat":"NULL"

X509 Certificate verification #14 (Valid Cert SHA1 Digest allowed in compile-time default profile)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBE
DTLS_PKCS1_V15:MBEDTLS_TLS_DEFAULT_ALLOW_SHA1_IN_CERTIFICATES
x509_verify:"data_files/cert_sha1.crt":"data_files/test-ca.crt":"data_files/crl.pem":"NULL":0:0:"default":"NULL"

X509 Certificate verification #14 (Valid Cert SHA1 Digest forbidden in default profile)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBE
DTLS_PKCS1_V15:!MBEDTLS_TLS_DEFAULT_ALLOW_SHA1_IN_CERTIFICATES
x509_verify:"data_files/cert_sha1.crt":"data_files/test-
ca.crt":"data_files/crl.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BAD
CRL_BAD_MD
| MBEDTLS_X509_BADCERT_BAD_MD:"default":"NULL"

X509 Certificate verification #15 (Valid Cert SHA224 Digest)
depends_on:MBEDTLS_SHA256_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MB
EDTLS_PKCS1_V15
x509_verify:"data_files/cert_sha224.crt":"data_files/test-
ca.crt":"data_files/crl.pem":"NULL":0:0:"compat":"NULL"

X509 Certificate verification #16 (Valid Cert SHA256 Digest)
depends_on:MBEDTLS_SHA256_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MB
EDTLS_PKCS1_V15
x509_verify:"data_files/cert_sha256.crt":"data_files/test-

ca.crt":"data_files/crl.pem":"NULL":0:0:"compat":"NULL"

X509 Certificate verification #17 (Valid Cert SHA384 Digest)
depends_on:MBEDTLS_SHA512_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_verify:"data_files/cert_sha384.crt":"data_files/test-ca.crt":"data_files/crl.pem":"NULL":0:0:"compat":"NULL"

X509 Certificate verification #18 (Valid Cert SHA512 Digest)
depends_on:MBEDTLS_SHA512_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_verify:"data_files/cert_sha512.crt":"data_files/test-ca.crt":"data_files/crl.pem":"NULL":0:0:"compat":"NULL"

X509
Certificate verification #19 (Valid Cert, denying callback)
depends_on:MBEDTLS_SHA512_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_verify:"data_files/cert_sha512.crt":"data_files/test-ca.crt":"data_files/crl.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_OTHER:"compat":"verify_none"

X509 Certificate verification #19 (Not trusted Cert, allowing callback)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15:MBEDTLS_SHA1_C
x509_verify:"data_files/server2.crt":"data_files/server1.crt":"data_files/crl_expired.pem":"NULL":0:0:"compat":"verify_all"

X509 Certificate verification #21 (domain matching wildcard certificate, case insensitive)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_verify:"data_files/cert_example_wildcard.crt":"data_files/test-ca.crt":"data_files/crl.pem":"mail.ExAmPlE.com":0:0:"compat":"NULL"

X509
Certificate verification #22 (domain not matching wildcard certificate)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_verify:"data_files/cert_example_wildcard.crt":"data_files/test-ca.crt":"data_files/crl.pem":"mail.example.net":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_CN_MISMATCH:"compat":"NULL"

X509 Certificate verification #23 (domain not matching wildcard certificate)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_verify:"data_files/cert_example_wildcard.crt":"data_files/test-ca.crt":"data_files/crl.pem":"example.com":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_CN_MISMATCH:"compat":"NULL"

X509 Certificate verification #24 (domain matching CN of multi certificate)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_verify:"data_files/cert_example_multi.crt":"data_files/test-

ca.crt":"data_files/crl.pem":"www.example.com":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_CN_MISMATCH:"compat":"NULL"

X509
Certificate verification #25 (domain matching multi certificate)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_verify:"data_files/cert_example_multi.crt":"data_files/test-ca.crt":"data_files/crl.pem":"example.net":0:0:"compat":"NULL"

X509 Certificate verification #26 (domain not matching multi certificate)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_verify:"data_files/cert_example_multi.crt":"data_files/test-ca.crt":"data_files/crl.pem":"www.example.net":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_CN_MISMATCH:"compat":"NULL"

X509 Certificate verification #27 (domain not matching multi certificate)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_verify:"data_files/cert_example_multi.crt":"data_files/test-ca.crt":"data_files/crl.pem":"xample.net":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_CN_MISMATCH:"compat":"NULL"

X509
Certificate verification #27 (domain not matching multi certificate)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_verify:"data_files/cert_example_multi.crt":"data_files/test-ca.crt":"data_files/crl.pem":"bexample.net":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_CN_MISMATCH:"compat":"NULL"

X509 Certificate verification #28 (domain not matching wildcard in multi certificate)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_verify:"data_files/cert_example_multi.crt":"data_files/test-ca.crt":"data_files/crl.pem":"example.org":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_CN_MISMATCH:"compat":"NULL"

X509 Certificate verification #29 (domain matching wildcard in multi certificate)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_verify:"data_files/cert_example_multi.crt":"data_files/test-ca.crt":"data_files/crl.pem":"mail.example.org":0:0:"compat":"NULL"

X509
Certificate verification #30 (domain matching multi certificate without CN)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_verify:"data_files/cert_example_multi_nocn.crt":"data_files/test-ca.crt":"data_files/crl.pem":"www.shotokan-braunschweig.de":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_NOT_TRUSTED:"compat":"NULL"

X509 Certificate verification #31 (domain not matching multi certificate without CN)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15

x509_verify:"data_files/cert_example_multi_nocn.crt":"data_files/test-ca.crt":"data_files/crl.pem":"www.example.net":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_CN_MISMATCH + MBEDTLS_X509_BADCERT_NOT_TRUSTED:"compat":"NULL"

X509 Certificate verification #32 (Valid, EC cert, RSA CA)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP192R1_ENABLED:MBEDTLS_PKCS1_V15:MBEDTLS_SHA1_C
x509_verify:"data_files/server3.crt":"data_files/test-ca.crt":"data_files/crl.pem":"NULL":0:0:"compat":"NULL"

X509
Certificate verification #33 (Valid, RSA cert, EC CA)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_ECP_C:MBEDTLS_SHA256_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_PKCS1_V15:MBEDTLS_ECP_DP_SECP384R1_ENABLED
x509_verify:"data_files/server4.crt":"data_files/test-ca2.crt":"data_files/crl-ec-sha256.pem":"NULL":0:0:"compat":"NULL"

X509 Certificate verification #34 (Valid, EC cert, EC CA)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_SHA256_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_ECP_DP_SECP384R1_ENABLED
x509_verify:"data_files/server5.crt":"data_files/test-ca2.crt":"data_files/crl-ec-sha256.pem":"NULL":0:0:"compat":"NULL"

X509 Certificate verification #35 (Revoked, EC CA)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_SHA256_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_ECP_DP_SECP384R1_ENABLED
x509_verify:"data_files/server6.crt":"data_files/test-ca2.crt":"data_files/crl-ec-sha256.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_REVOKED:"compat":"NULL"

X509
Certificate verification #36 (Valid, EC CA, SHA1 Digest)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_SHA256_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA1_C
x509_verify:"data_files/server5-sha1.crt":"data_files/test-ca2.crt":"data_files/crl-ec-sha256.pem":"NULL":0:0:"compat":"NULL"

X509 Certificate verification #37 (Valid, EC CA, SHA224 Digest)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_SHA256_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_ECP_DP_SECP384R1_ENABLED
x509_verify:"data_files/server5-sha224.crt":"data_files/test-ca2.crt":"data_files/crl-ec-sha256.pem":"NULL":0:0:"compat":"NULL"

X509 Certificate verification #38 (Valid, EC CA, SHA384 Digest)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_SHA256_C:MBEDTLS_SHA512_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_ECP_DP_SECP384R1_ENABLED
x509_verify:"data_files/server5-sha384.crt":"data_files/test-ca2.crt":"data_files/crl-ec-sha256.pem":"NULL":0:0:"compat":"NULL"

X509
Certificate verification #39 (Valid, EC CA, SHA512 Digest)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_SHA256_C:MBEDTLS_SHA512_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_ECP_DP_SECP384R1_ENABLED
x509_verify:"data_files/server5-sha512.crt":"data_files/test-ca2.crt":"data_files/crl-ec-sha256.pem":"NULL":0:0:"compat":"NULL"

X509 Certificate verification #40 (Valid, depth 0, RSA, CA)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15:MBEDTLS_SHA256_C:MBEDTLS_SHA1_C
x509_verify:"data_files/test-ca.crt":"data_files/test-ca.crt":"data_files/crl.pem":"NULL":0:0:"compat":"NULL"

X509 Certificate verification #41 (Valid, depth 0, EC, CA)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA256_C
x509_verify:"data_files/test-ca2.crt":"data_files/test-ca2.crt":"data_files/crl-ec-sha256.pem":"NULL":0:0:"compat":"NULL"

X509
Certificate verification #42 (Depth 0, not CA, RSA)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15:MBEDTLS_SHA1_C
x509_verify:"data_files/server2.crt":"data_files/server2.crt":"data_files/crl.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_NOT_TRUSTED:"compat":"NULL"

X509 Certificate verification #43 (Depth 0, not CA, EC)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECDSA_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA256_C
x509_verify:"data_files/server5.crt":"data_files/server5.crt":"data_files/crl-ec-sha256.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_NOT_TRUSTED:"compat":"NULL"

X509 Certificate verification #44 (Corrupted signature, EC)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA256_C
x509_verify:"data_files/server5-badsign.crt":"data_files/test-ca2.crt":"data_files/crl-ec-sha256.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_NOT_TRUSTED:"compat":"NULL"

X509
Certificate verification #45 (Corrupted signature, RSA)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15:MBEDTLS_SHA1_C
x509_verify:"data_files/server2-badsign.crt":"data_files/test-ca.crt":"data_files/crl.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_NOT_TRUSTED:"compat":"NULL"

X509 Certificate verification #46 (Valid, depth 2, EC-RSA-EC)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECDSA_C:MBEDTLS_RSA_C:MBEDTLS_ECP_DP_SE

CP256R1_ENABLED:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_PKCS1_V15:MBEDTLS_SHA256_C
x509_verify:"data_files/server7_int-ca.crt":"data_files/test-ca2.crt":"data_files/crl-ec-sha256.pem":"NULL":0:0:"compat":"NULL"

X509 Certificate verification #47 (Untrusted, depth 2, EC-RSA-EC)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECDSA_C:MBEDTLS_RSA_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_PKCS1_V15:MBEDTLS_SHA1_C:MBEDTLS_SHA256_C
x509_verify:"data_files/server7_int-ca.crt":"data_files/test-ca.crt":"data_files/crl-ec-sha256.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_NOT_TRUSTED:"compat":"NULL"

X509
Certificate verification #48 (Missing intermediate CA, EC-RSA-EC)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECDSA_C:MBEDTLS_RSA_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_PKCS1_V15:MBEDTLS_SHA1_C:MBEDTLS_SHA256_C
x509_verify:"data_files/server7.crt":"data_files/test-ca.crt":"data_files/crl-ec-sha256.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_NOT_TRUSTED:"compat":"NULL"

X509 Certificate verification #49 (Valid, depth 2, RSA-EC-RSA)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECDSA_C:MBEDTLS_RSA_C:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_PKCS1_V15:MBEDTLS_SHA256_C:MBEDTLS_SHA1_C
x509_verify:"data_files/server8_int-ca2.crt":"data_files/test-ca.crt":"data_files/crl-ec-sha256.pem":"NULL":0:0:"compat":"NULL"

X509 Certificate verification
#50 (Valid, multiple CAs)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA1_C:MBEDTLS_SHA256_C
x509_verify:"data_files/server2.crt":"data_files/test-ca_cat12.crt":"data_files/crl.pem":"NULL":0:0:"compat":"NULL"

X509 Certificate verification #51 (Valid, multiple CAs, reverse order)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA1_C:MBEDTLS_SHA256_C
x509_verify:"data_files/server2.crt":"data_files/test-ca_cat21.crt":"data_files/crl.pem":"NULL":0:0:"compat":"NULL"

X509 Certificate verification #52 (CA keyUsage valid)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECDSA_C:MBEDTLS_SHA256_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_ECP_DP_SECP384R1_ENABLED
x509_verify:"data_files/server5.crt":"data_files/test-ca2.ku-crt_crl.crt":"data_files/crl-ec-sha256.pem":"NULL":0:0:"compat":"NULL"

X509 Certificate verification #53 (CA keyUsage missing cRLSign)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECDSA_C:MBEDTLS_SHA256_C:MBEDTLS_X509_CHECK_KEY_USAGE:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_ECP_DP_SECP384R1_ENABL

ED
x509_verify:"data_files/server5.crt":"data_files/test-ca2.ku-crt.crt":"data_files/crl-ec-sha256.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCRL_NOT_TRUSTED:"compat":"NULL"

X509
Certificate verification #54 (CA keyUsage missing cRLSign, no CRL)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECDSA_C:MBEDTLS_SHA256_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA1_C
x509_verify:"data_files/server5.crt":"data_files/test-ca2.ku-crt.crt":"data_files/crl.pem":"NULL":0:0:"compat":"NULL"

X509 Certificate verification #55 (CA keyUsage missing keyCertSign)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECDSA_C:MBEDTLS_SHA256_C:MBEDTLS_X509_CHECK_KEY_USAGE:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_ECP_DP_SECP384R1_ENABLED
x509_verify:"data_files/server5.crt":"data_files/test-ca2.ku-crl.crt":"data_files/crl-ec-sha256.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_NOT_TRUSTED:"compat":"NULL"

X509
Certificate verification #56 (CA keyUsage plain wrong)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECDSA_C:MBEDTLS_SHA256_C:MBEDTLS_X509_CHECK_KEY_USAGE:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_ECP_DP_SECP384R1_ENABLED
x509_verify:"data_files/server5.crt":"data_files/test-ca2.ku-ds.crt":"data_files/crl-ec-sha256.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_NOT_TRUSTED:"compat":"NULL"

X509 Certificate verification #57 (Valid, RSASSA-PSS, SHA-1)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_X509_RSASSA_PSS_SUPPORT:MBEDTLS_SHA1_C
x509_verify:"data_files/server9.crt":"data_files/test-ca.crt":"data_files/crl.pem":"NULL":0:0:"compat":"NULL"

X509 Certificate verification #58 (Valid, RSASSA-PSS, SHA-224)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_X509_RSASSA_PSS_SUPPORT:MBEDTLS_SHA256_C:MBEDTLS_SHA1_C
x509_verify:"data_files/server9-sha224.crt":"data_files/test-ca.crt":"data_files/crl-rsa-pss-sha224.pem":"NULL":0:0:"compat":"NULL"

X509
Certificate verification #59 (Valid, RSASSA-PSS, SHA-256)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_X509_RSASSA_PSS_SUPPORT:MBEDTLS_SHA256_C:MBEDTLS_SHA1_C
x509_verify:"data_files/server9-sha256.crt":"data_files/test-ca.crt":"data_files/crl-rsa-pss-sha256.pem":"NULL":0:0:"compat":"NULL"

X509 Certificate verification #60 (Valid, RSASSA-PSS, SHA-384)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_X509_RSASSA_PSS_SUPPORT:MBEDTLS_SHA512_C:

MBEDTLS_SHA1_C
x509_verify:"data_files/server9-sha384.crt":"data_files/test-ca.crt":"data_files/crl-rsa-pss-sha384.pem":"NULL":0:0:"compat":"NULL"

X509 Certificate verification #61 (Valid, RSASSA-PSS, SHA-512)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_X509_RSASSA_PSS_SUPPORT:MBEDTLS_SHA512_C:MBEDTLS_SHA1_C
x509_verify:"data_files/server9-sha512.crt":"data_files/test-ca.crt":"data_files/crl-rsa-pss-sha512.pem":"NULL":0:0:"compat":"NULL"

X509 Certificate verification #62 (Revoked, RSASSA-PSS, SHA-1)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_X509_RSASSA_PSS_SUPPORT:MBEDTLS_SHA1_C
x509_verify:"data_files/server9.crt":"data_files/test-ca.crt":"data_files/crl-rsa-pss-sha1.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_REVOKED:"compat":"NULL"

X509
Certificate verification #63 (Revoked, RSASSA-PSS, SHA-1, CRL badsign)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_X509_RSASSA_PSS_SUPPORT:MBEDTLS_SHA1_C
x509_verify:"data_files/server9.crt":"data_files/test-ca.crt":"data_files/crl-rsa-pss-sha1-badsign.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCRL_NOT_TRUSTED:"compat":"NULL"

X509 Certificate verification #64 (Valid, RSASSA-PSS, SHA-1, not top)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_X509_RSASSA_PSS_SUPPORT:MBEDTLS_SHA1_C
x509_verify:"data_files/server9-with-ca.crt":"data_files/test-ca.crt":"data_files/crl.pem":"NULL":0:0:"compat":"NULL"

X509 Certificate verification #65 (RSASSA-PSS, SHA1, bad cert signature)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_X509_RSASSA_PSS_SUPPORT:MBEDTLS_SHA1_C
x509_verify:"data_files/server9-badsign.crt":"data_files/test-ca.crt":"data_files/crl.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_NOT_TRUSTED:"compat":"NULL"

X509
Certificate verification #66 (RSASSA-PSS, SHA1, no RSA CA)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_X509_RSASSA_PSS_SUPPORT:MBEDTLS_SHA1_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA256_C
x509_verify:"data_files/server9.crt":"data_files/test-ca2.crt":"data_files/crl.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_NOT_TRUSTED:"compat":"NULL"

X509 Certificate verification #67 (Valid, RSASSA-PSS, all defaults)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_X509_RSASSA_PSS_SUPPORT:MBEDTLS_SHA1_C
x509_verify:"data_files/server9-defaults.crt":"data_files/test-ca.crt":"data_files/crl-rsa-pss-sha1.pem":"NULL":0:0:"compat":"NULL"

X509 Certificate verification #68 (RSASSA-PSS, wrong salt_len)

depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_X509_RSASSA_PSS_SUPPORT:MBEDTLS_SHA256_C:MBEDTLS_SHA1_C
x509_verify:"data_files/server9-bad-saltlen.crt":"data_files/test-ca.crt":"data_files/crl.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_NOT_TRUSTED:"compat":"NULL"

X509
Certificate verification #69 (RSASSA-PSS, wrong mgf_hash)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_X509_RSASSA_PSS_SUPPORT:MBEDTLS_SHA256_C:MBEDTLS_SHA1_C
x509_verify:"data_files/server9-bad-mgfhash.crt":"data_files/test-ca.crt":"data_files/crl.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_NOT_TRUSTED:"compat":"NULL"

X509 Certificate verification #70 (v1 trusted CA)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15:MBEDTLS_SHA256_C:MBEDTLS_SHA1_C
x509_verify:"data_files/server1-v1.crt":"data_files/test-ca-v1.crt":"data_files/crl.pem":"NULL":0:0:"compat":"NULL"

X509 Certificate verification #71 (v1 trusted CA, other)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15:MBEDTLS_SHA256_C:MBEDTLS_SHA1_C
x509_verify:"data_files/server2-v1.crt":"data_files/server1-v1.crt":"data_files/crl.pem":"NULL":0:0:"compat":"NULL"

X509
Certificate verification #72 (v1 chain)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15:MBEDTLS_SHA256_C:MBEDTLS_SHA1_C
x509_verify:"data_files/server2-v1-chain.crt":"data_files/test-ca-v1.crt":"data_files/crl.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_NOT_TRUSTED:"compat":"NULL"

X509 Certificate verification #73 (selfsigned trusted without CA bit)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECDSA_C:MBEDTLS_SHA256_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA1_C
x509_verify:"data_files/server5-selfsigned.crt":"data_files/server5-selfsigned.crt":"data_files/crl.pem":"NULL":0:0:"compat":"NULL"

X509 Certificate verification #74 (signed by selfsigned trusted without CA bit)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECDSA_C:MBEDTLS_SHA256_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA1_C
x509_verify:"data_files/server6-ss-child.crt":"data_files/server5-selfsigned.crt":"data_files/crl.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_NOT_TRUSTED:"compat":"NULL"

X509

Certificate verification #75 (encoding mismatch)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C
x509_verify:"data_files/enco-cert-utf8str.pem":"data_files/enco-ca-
prstr.pem":"data_files/crl.pem":"NULL":0:0:"compat":"NULL"

X509 Certificate verification #76 (multiple CRLs, not revoked)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECDSA_C:MBEDTLS_ECP_DP_SECP384R1_ENABLED
:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA256_C:MBEDTLS_RSA_C:MBEDTLS_SHA1
_C
x509_verify:"data_files/server5.crt":"data_files/test-ca_cat12.crt":"data_files/crl_cat_ec-
rsa.pem":"NULL":0:0:"compat":"NULL"

X509 Certificate verification #77 (multiple CRLs, revoked)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECDSA_C:MBEDTLS_ECP_DP_SECP384R1_ENABLED
:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA256_C:MBEDTLS_RSA_C:MBEDTLS_SHA1
_C
x509_verify:"data_files/server6.crt":"data_files/test-ca_cat12.crt":"data_files/crl_cat_ec-
rsa.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_REVOKED
:"compat":"NULL"

X509
Certificate verification #78 (multiple CRLs, revoked by second)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECDSA_C:MBEDTLS_ECP_DP_SECP384R1_ENABLED
:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA256_C:MBEDTLS_RSA_C:MBEDTLS_SHA1
_C
x509_verify:"data_files/server6.crt":"data_files/test-ca_cat12.crt":"data_files/crl_cat_rsa-
ec.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_REVOKED:
"compat":"NULL"

X509 Certificate verification #79 (multiple CRLs, revoked by future)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECDSA_C:MBEDTLS_ECP_DP_SECP384R1_ENABLED
:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA256_C:MBEDTLS_RSA_C:MBEDTLS_SHA1
_C
x509_verify:"data_files/server6.crt":"data_files/test-ca_cat12.crt":"data_files/crl_cat_ecfut-
rsa.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_REVOKED
|MBEDTLS_X509_BADCRL_FUTURE:"compat":"NULL"

X509 Certificate verification
#80 (multiple CRLs, first future, revoked by second)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECDSA_C:MBEDTLS_ECP_DP_SECP384R1_ENABLED
:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA256_C:MBEDTLS_RSA_C:MBEDTLS_SHA1
_C
x509_verify:"data_files/server1.crt":"data_files/test-ca_cat12.crt":"data_files/crl_cat_ecfut-
rsa.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_REVOKED
:"compat":"NULL"

X509 Certificate verification #81 (multiple CRLs, none relevant)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECDSA_C:MBEDTLS_ECP_DP_SECP384R1_ENABLED

:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA256_C:MBEDTLS_RSA_C:MBEDTLS_SHA1
_C
x509_verify:"data_files/enco-cert-utf8str.pem":"data_files/enco-ca-prstr.pem":"data_files/crl_cat_rsa-
ec.pem":"NULL":0:0:"compat":"NULL"

X509 Certificate verification #82 (Not yet valid CA and valid CA)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:M
BEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA1_C:MBEDTLS_SHA256_C
x509_verify:"data_files/server5.crt":"data_files/test-ca2_cat-future-present.crt":"data_files/crl-ec-
sha1.pem":"NULL":0:0:"compat":"NULL"

X509
Certificate verification #83 (valid CA and Not yet valid CA)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:M
BEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA1_C:MBEDTLS_SHA256_C
x509_verify:"data_files/server5.crt":"data_files/test-ca2_cat-present-future.crt":"data_files/crl-ec-
sha1.pem":"NULL":0:0:"compat":"NULL"

X509 Certificate verification #84 (valid CA and Not yet valid CA)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:M
BEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA1_C:MBEDTLS_SHA256_C
x509_verify:"data_files/server5.crt":"data_files/test-ca2_cat-present-past.crt":"data_files/crl-ec-
sha1.pem":"NULL":0:0:"compat":"NULL"

X509 Certificate verification #85 (Not yet valid CA and valid CA)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:M
BEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA1_C:MBEDTLS_SHA256_C
x509_verify:"data_files/server5.crt":"data_files/test-ca2_cat-past-present.crt":"data_files/crl-ec-
sha1.pem":"NULL":0:0:"compat":"NULL"

X509
Certificate verification #86 (Not yet valid CA and invalid CA)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:M
BEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA1_C:MBEDTLS_SHA256_C
x509_verify:"data_files/server5.crt":"data_files/test-ca2_cat-future-invalid.crt":"data_files/crl-ec-
sha1.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_FUTURE
:"compat":"NULL"

X509 Certificate verification #87 (Expired CA and invalid CA)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:M
BEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA1_C:MBEDTLS_SHA256_C
x509_verify:"data_files/server5.crt":"data_files/test-ca2_cat-past-invalid.crt":"data_files/crl-ec-
sha1.pem":"NULL":MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_EXPIRE
D:"compat":"NULL"

X509 Certificate verification
callback: trusted EE cert
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECDSA_C:MBEDTLS_SHA256_C:MBEDTLS_ECP_DP_

SECP256R1_ENABLED
x509_verify_callback:"data_files/server5-selfsigned.crt":"data_files/server5-selfsigned.crt":0:"depth 0 - serial 53\:A2\:CB\:4B\:12\:4E\:AD\:83\:7D\:A8\:94\:B2 - subject CN=selfsigned, OU=testing, O=PolarSSL, C=NL\n"

X509 Certificate verification callback: simple
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_verify_callback:"data_files/server1.crt":"data_files/test-ca.crt":0:"depth 1 - serial 00 - subject C=NL, O=PolarSSL, CN=PolarSSL Test CA\ndepth 0 - serial 01 - subject C=NL, O=PolarSSL, CN=PolarSSL Server 1\n"

X509 Certificate verification callback: two trusted roots
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15:MBEDTLS_ECDSA_C:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA256_C
x509_verify_callback:"data_files/server1.crt":"data_files/test-ca_cat12.crt":0:"depth 1 - serial 00 - subject C=NL, O=PolarSSL, CN=PolarSSL Test CA\ndepth 0 - serial 01 - subject C=NL, O=PolarSSL, CN=PolarSSL Server 1\n"

X509 Certificate verification callback: two trusted roots, reversed order
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15:MBEDTLS_ECDSA_C:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA256_C
x509_verify_callback:"data_files/server1.crt":"data_files/test-ca_cat21.crt":0:"depth 1 - serial 00 - subject C=NL, O=PolarSSL, CN=PolarSSL Test CA\ndepth 0 - serial 01 - subject C=NL, O=PolarSSL, CN=PolarSSL Server 1\n"

X509 Certificate verification callback: root included
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15:MBEDTLS_ECDSA_C:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA256_C
x509_verify_callback:"data_files/server1_ca.crt":"data_files/test-ca_cat21.crt":0:"depth 1 - serial 00 - subject C=NL, O=PolarSSL, CN=PolarSSL Test CA\ndepth 0 - serial 01 - subject C=NL, O=PolarSSL, CN=PolarSSL Server 1\n"

X509 Certificate verification
callback: intermediate ca
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECDSA_C:MBEDTLS_RSA_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_PKCS1_V15:MBEDTLS_SHA256_C:MBEDTLS_SHA1_C
x509_verify_callback:"data_files/server7_int-ca.crt":"data_files/test-ca_cat12.crt":0:"depth 2 - serial C1\:43\:E2\:7E\:62\:43\:CC\:E8 - subject C=NL, O=PolarSSL, CN=Polarssl Test EC CA\ndepth 1 - serial 0E - subject C=NL, O=PolarSSL, CN=PolarSSL Test Intermediate CA\ndepth 0 - serial 10 - subject C=NL, O=PolarSSL, CN=localhost\n"

X509 Certificate verification callback: intermediate ca, root included
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECDSA_C:MBEDTLS_RSA_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_PKCS1_V15:MBEDTLS_SHA256_C:MBEDTLS_SHA1_C
x509_verify_callback:"data_files/server7_int-ca_ca2.crt":"data_files/test-ca_cat12.crt":0:"depth 2 - serial C1\:43\:E2\:7E\:62\:43\:CC\:E8 - subject C=NL, O=PolarSSL, CN=Polarssl Test EC CA\ndepth 1 - serial 0E - subject C=NL, O=PolarSSL, CN=PolarSSL Test Intermediate CA\ndepth 0 - serial 10 - subject C=NL, O=PolarSSL, CN=localhost\n"

X509 Certificate verification callback: intermediate ca trusted
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECDSA_C:MBEDTLS_RSA_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_PKCS1_V15:MBEDTLS_SHA256_C
x509_verify_callback:"data_files/server7_int-ca_ca2.crt":"data_files/test-int-ca.crt":0:"depth 1 - serial 0E - subject C=NL, O=PolarSSL, CN=PolarSSL Test Intermediate CA\ndepth 0 - serial 10 - subject C=NL, O=PolarSSL, CN=localhost\n"

X509 Certificate verification callback: two intermediates
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECDSA_C:MBEDTLS_RSA_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_PKCS1_V15:MBEDTLS_SHA256_C:MBEDTLS_SHA1_C
x509_verify_callback:"data_files/server10_int3_int-ca2.crt":"data_files/test-ca_cat21.crt":0:"depth 3 - serial 00 - subject C=NL, O=PolarSSL, CN=PolarSSL Test CA\ndepth 2 -
serial 0F - subject C=NL, O=PolarSSL, CN=PolarSSL Test Intermediate EC CA\ndepth 1 - serial 4D - subject C=UK, O=mbed TLS, CN=mbed TLS Test intermediate CA 3\ndepth 0 - serial 4B - subject CN=localhost\n"

X509 Certificate verification callback: two intermediates, root included
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECDSA_C:MBEDTLS_RSA_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_PKCS1_V15:MBEDTLS_SHA256_C:MBEDTLS_SHA1_C
x509_verify_callback:"data_files/server10_int3_int-ca2_ca.crt":"data_files/test-ca_cat21.crt":0:"depth 3 - serial 00 - subject C=NL, O=PolarSSL, CN=PolarSSL Test CA\ndepth 2 - serial 0F - subject C=NL, O=PolarSSL, CN=PolarSSL Test Intermediate EC CA\ndepth 1 - serial 4D - subject C=UK, O=mbed TLS, CN=mbed TLS Test intermediate CA 3\ndepth 0 - serial 4B - subject CN=localhost\n"

X509 Certificate verification callback: two intermediates, top int trusted
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECDSA_C:MBEDTLS_RSA_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_PKCS1_V15:MBEDTLS_SHA256_C
x509_verify_callback:"data_files/server10_int3_int-ca2.crt":"data_files/test-int-ca2.crt":0:"depth
2 - serial 0F - subject C=NL, O=PolarSSL, CN=PolarSSL Test Intermediate EC CA\ndepth 1 - serial 4D - subject C=UK, O=mbed TLS, CN=mbed TLS Test intermediate CA 3\ndepth 0 - serial 4B - subject CN=localhost\n"

X509 Certificate verification callback: two intermediates, low int trusted
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECDSA_C:MBEDTLS_RSA_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_PKCS1_V15:MBEDTLS_SHA256_C:MBEDTLS_SHA1_C
x509_verify_callback:"data_files/server10_int3_int-ca2_ca.crt":"data_files/test-int-ca3.crt":0:"depth 1 - serial 4D - subject C=UK, O=mbed TLS, CN=mbed TLS Test intermediate CA 3\ndepth 0 - serial 4B - subject CN=localhost\n"

X509 Parse Selftest
depends_on:MBEDTLS_SHA1_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_CERTS_C
x509_selftest:

X509 Certificate ASN1 (Incorrect first

tag)
x509parse_crt:"":"":MBEDTLS_ERR_X509_INVALID_FORMAT

X509 Certificate ASN1 (Correct first tag, data length does not match)
x509parse_crt:"300000":"":MBEDTLS_ERR_X509_INVALID_FORMAT +
MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 Certificate ASN1 (Correct first tag, no more data)
x509parse_crt:"3000":"":MBEDTLS_ERR_X509_INVALID_FORMAT +
MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 Certificate ASN1 (Correct first tag, length data incorrect)
x509parse_crt:"30023085":"":MBEDTLS_ERR_X509_INVALID_FORMAT +
MBEDTLS_ERR_ASN1_INVALID_LENGTH

X509 Certificate ASN1 (Correct first tag, length data incomplete)
x509parse_crt:"30023083":"":MBEDTLS_ERR_X509_INVALID_FORMAT +
MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 Certificate ASN1 (Correct first tag, length data incomplete)
x509parse_crt:"30023081":"":MBEDTLS_ERR_X509_INVALID_FORMAT +
MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 Certificate ASN1 (Correct first tag, length data incomplete)
x509parse_crt:"3003308200":"":MBEDTLS_ERR_X509_INVALID_FORMAT +
MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509
Certificate ASN1 (Correct first tag, second tag no TBSCertificate)
x509parse_crt:"300100":"":MBEDTLS_ERR_X509_INVALID_FORMAT +
MBEDTLS_ERR_ASN1_UNEXPECTED_TAG

X509 Certificate ASN1 (TBSCertificate, no version tag, serial missing)
x509parse_crt:"3003300100":"":MBEDTLS_ERR_X509_INVALID_SERIAL +
MBEDTLS_ERR_ASN1_UNEXPECTED_TAG

X509 Certificate ASN1 (TBSCertificate, invalid version tag)
x509parse_crt:"30053003a00101":"":MBEDTLS_ERR_X509_INVALID_VERSION +
MBEDTLS_ERR_ASN1_UNEXPECTED_TAG

X509 Certificate ASN1 (TBSCertificate, valid version tag, no length)
x509parse_crt:"30053003a00102":"":MBEDTLS_ERR_X509_INVALID_VERSION +
MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 Certificate ASN1 (TBSCertificate, valid version tag, invalid length)
x509parse_crt:"30163014a012021000000000000000000000000000000000":"":MBEDTLS_ERR_X509_INVALID
_VERSION + MBEDTLS_ERR_ASN1_INVALID_LENGTH

X509 Certificate ASN1 (TBSCertificate, valid version tag, no serial)
x509parse_crt:"30073005a003020104":"":MBEDTLS_ERR_X509_INVALID_SERIAL
+ MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 Certificate ASN1 (TBSCertificate, invalid length version tag)
x509parse_crt:"30083006a00402010400":"":MBEDTLS_ERR_X509_INVALID_VERSION +
MBEDTLS_ERR_ASN1_LENGTH_MISMATCH

X509 Certificate ASN1 (TBSCertificate, incorrect serial tag)
x509parse_crt:"30083006a00302010400":"":MBEDTLS_ERR_X509_INVALID_SERIAL +
MBEDTLS_ERR_ASN1_UNEXPECTED_TAG

X509 Certificate ASN1 (TBSCertificate, incorrect serial length)
x509parse_crt:"30083006a00302010482":"":MBEDTLS_ERR_X509_INVALID_SERIAL +
MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 Certificate ASN1 (TBSCertificate, correct serial, no alg)
x509parse_crt:"300d300ba0030201048204deadbeef":"":MBEDTLS_ERR_X509_INVALID_ALG +
MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 Certificate ASN1 (TBSCertificate, correct serial, no alg oid)
x509parse_crt:"300e300ca0030201048204deadbeef00":"":MBEDTLS_ERR_X509_INVALID_ALG +
MBEDTLS_ERR_ASN1_UNEXPECTED_TAG

X509 Certificate ASN1 (TBSCertificate, alg oid no data in sequence)
x509parse_crt:"300f300da0030201048204deadbeef3000":"":MBEDTLS_ERR_X509_INVALID_ALG
+ MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 Certificate ASN1 (TBSCertificate, alg with params)
x509parse_crt:"30163014a0030201048204deadbeef30070604cafed00d01":"":MBEDTLS_ERR_X509_INVALID_
ALG + MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 Certificate ASN1 (TBSCertificate, correct alg data, no params unknown version)
x509parse_crt:"30153013a0030201048204deadbeef30060604cafed00d":"":MBEDTLS_ERR_X509_UNKNOWN_
VERSION

X509 Certificate ASN1 (TBSCertificate, correct alg data, unknown version)
x509parse_crt:"30173015a0030201048204deadbeef30080604cafed00d0500":"":MBEDTLS_ERR_X509_UNKNO
WN_VERSION

X509 Certificate ASN1 (TBSCertificate, correct alg data, length mismatch)
x509parse_crt:"30183016a0030201048204deadbeef30090604cafed00d050000":"":MBEDTLS_ERR_X509_INVAL
ID_ALG + MBEDTLS_ERR_ASN1_LENGTH_MISMATCH

X509 Certificate ASN1 (TBSCertificate, correct alg, unknown alg_id)
x509parse_crt:"30173015a0030201028204deadbeef30080604cafed00d0500":"":MBEDTLS_ERR_X509_UNKNO
WN_SIG_ALG

+ MBEDTLS_ERR_OID_NOT_FOUND

X509 Certificate ASN1 (TBSCertificate, correct alg, specific alg_id)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"301c301aa0030201028204deadbeef300d06092a864886f70d0101020500":"":MBEDTLS_ERR_X509_INVALID_FORMAT + MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 Certificate ASN1 (TBSCertificate, correct alg, unknown specific alg_id)
x509parse_crt:"301c301aa0030201028204deadbeef300d06092a864886f70d0101010500":"":MBEDTLS_ERR_X509_UNKNOWN_SIG_ALG + MBEDTLS_ERR_OID_NOT_FOUND

X509 Certificate ASN1 (TBSCertificate, correct alg, bad RSASSA-PSS params)
depends_on:MBEDTLS_X509_RSASSA_PSS_SUPPORT
x509parse_crt:"30193017A003020102020118300D06092A864886F70D01010A3100":"":MBEDTLS_ERR_X509_INVALID_ALG + MBEDTLS_ERR_ASN1_UNEXPECTED_TAG

X509 Certificate ASN1 (TBSCertificate, issuer no set data)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"301e301ca0030201028204deadbeef300d06092a864886f70d01010205003000":"":MBEDTLS_ERR_X509_INVALID_NAME + MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509
Certificate ASN1 (TBSCertificate, issuer no inner seq data)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"3020301ea0030201028204deadbeef300d06092a864886f70d010102050030023100":"":MBEDTLS_ERR_X509_INVALID_NAME + MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 Certificate ASN1 (TBSCertificate, issuer no inner set data)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"30223020a0030201028204deadbeef300d06092a864886f70d0101020500300431023000":"":MBEDTLS_ERR_X509_INVALID_NAME + MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 Certificate ASN1 (TBSCertificate, issuer two inner set datas)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"30243022a0030201028204deadbeef300d06092a864886f70d0101020500300631043000300":"":MBEDTLS_ERR_X509_INVALID_NAME + MBEDTLS_ERR_ASN1_UNEXPECTED_TAG

X509 Certificate ASN1 (TBSCertificate, issuer no oid data)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"30243022a0030201028204deadbeef300d06092a864886f70d0101020500300631043002060":"":MBEDTLS_ERR_X509_INVALID_NAME
+ MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 Certificate ASN1 (TBSCertificate, issuer invalid tag)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"302a3028a0030201028204deadbeef300d06092a864886f70d0101020500300c310a300806000604546573374":"":MBEDTLS_ERR_X509_INVALID_NAME + MBEDTLS_ERR_ASN1_UNEXPECTED_TAG

X509 Certificate ASN1 (TBSCertificate, issuer, no string data)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"30253023a0030201028204deadbeef300d06092a864886f70d0101020500300731053003060013":"":
MBEDTLS_ERR_X509_INVALID_NAME + MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 Certificate ASN1 (TBSCertificate, issuer, no full following string)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"302b3029a0030201028204deadbeef300d06092a864886f70d0101020500300d310b30090600130454
65737400":"":MBEDTLS_ERR_X509_INVALID_NAME+MBEDTLS_ERR_ASN1_UNEXPECTED_TAG

X509 Certificate ASN1 (TBSCertificate, valid issuer, no validity)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"302a3028a0030201028204deadbeef300d06092a864886f70d0101020500300c310a30080600130454
657374":"":MBEDTLS_ERR_X509_INVALID_DATE
+ MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 Certificate ASN1 (TBSCertificate, too much date data)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"30493047a0030201028204deadbeef300d06092a864886f70d0101020500300c310a30080600130454
657374301d170c303930313031303030303030170c303931323331323335393539300":"":MBEDTLS_ERR_X509_I
NVALID_DATE + MBEDTLS_ERR_ASN1_LENGTH_MISMATCH

X509 Certificate ASN1 (TBSCertificate, invalid from date)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"30483046a0030201028204deadbeef300d06092a864886f70d0101020500300c310a30080600130454
657374301c170c303930313031303000000000170c303931323331323300000000":"":MBEDTLS_ERR_X509_INV
ALID_DATE

X509 Certificate ASN1 (TBSCertificate, invalid to date)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"30483046a0030201028204deadbeef300d06092a864886f70d0101020500300c310a30080600130454
657374301c170c303930313031303030303030170c303931323331323300000000":"":MBEDTLS_ERR_X509_INV
ALID_DATE

X509
Certificate ASN1 (TBSCertificate, valid validity, no subject)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"30493047a0030201028204deadbeef300d06092a864886f70d0101020500300c310a30080600130454
657374301c170c303930313031303030303030170c303931323331323335393539330":"":MBEDTLS_ERR_X509_I
NVALID_FORMAT + MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 Certificate ASN1 (TBSCertificate, valid subject, no pubkeyinfo)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"30563054a0030201028204deadbeef300d06092a864886f70d0101020500300c310a30080600130454
657374301c170c303930313031303030303030170c303931323331323335393539300c310a30080600130454657374
":"":MBEDTLS_ERR_PK_KEY_INVALID_FORMAT + MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 Certificate ASN1 (TBSCertificate, pubkey, no alg)

depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"30583056a0030201028204deadbeef300d06092a864886f70d0101020500300c310a30080600130454
657374301c170c3039303130313030303030170c3039313233313233353935393300c310a30080600130454657374
3000":"":MBEDTLS_ERR_PK_INVALID_ALG
+ MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 Certificate ASN1 (TBSCertificate, valid subject, unknown pk alg)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"30673065a0030201028204deadbeef300d06092a864886f70d0101020500300c310a30080600130454
657374301c170c3039303130313030303030170c3039313233313233353935393300c310a30080600130454657374
300f300d06092A864886F70D0101000500":"":MBEDTLS_ERR_PK_UNKNOWN_PK_ALG

X509 Certificate ASN1 (TBSCertificate, pubkey, no bitstring)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"30673065a0030201028204deadbeef300d06092a864886f70d0101020500300c310a30080600130454
657374301c170c3039303130313030303030170c3039313233313233353935393300c310a30080600130454657374
300f300d06092A864886F70D0101010500":"":MBEDTLS_ERR_PK_INVALID_PUBKEY +
MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 Certificate ASN1 (TBSCertificate, pubkey, no bitstring data)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"30693067a0030201028204deadbeef300d06092a864886f70d0101020500300c310a30080600130454
657374301c170c3039303130313030303030170c3039313233313233353935393300c310a30080600130454657374
3011300d06092A864886F70D01010105000300":"":MBEDTLS_ERR_PK_INVALID_PUBKEY
+ MBEDTLS_ERR_ASN1_INVALID_DATA

X509 Certificate ASN1 (TBSCertificate, pubkey, invalid bitstring start)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"306a3068a0030201028204deadbeef300d06092a864886f70d0101020500300c310a30080600130454
657374301c170c3039303130313030303030170c3039313233313233353935393300c310a30080600130454657374
3012300d06092A864886F70D0101010500030101":"":MBEDTLS_ERR_PK_INVALID_PUBKEY +
MBEDTLS_ERR_ASN1_INVALID_DATA

X509 Certificate ASN1 (TBSCertificate, pubkey, invalid internal bitstring length)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"306d306ba0030201028204deadbeef300d06092a864886f70d0101020500300c310a30080600130454
657374301c170c3039303130313030303030170c3039313233313233353935393300c310a30080600130454657374
3015300d06092A864886F70D010101050003040030000":"":MBEDTLS_ERR_PK_INVALID_PUBKEY
+ MBEDTLS_ERR_ASN1_LENGTH_MISMATCH

X509 Certificate ASN1 (TBSCertificate, pubkey, invalid internal bitstring tag)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"306d306ba0030201028204deadbeef300d06092a864886f70d0101020500300c310a30080600130454
657374301c170c3039303130313030303030170c3039313233313233353935393300c310a30080600130454657374
3015300d06092A864886F70D010101050003040031000":"":MBEDTLS_ERR_PK_INVALID_PUBKEY +
MBEDTLS_ERR_ASN1_UNEXPECTED_TAG

X509 Certificate ASN1 (TBSCertificate, pubkey, invalid mbedtls_mpi)

depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"30743072a0030201028204deadbeef300d06092a864886f70d0101020500300c310a30080600130454
657374301c170c3039303130313030303030170c3039313233313233335393539300c310a30080600130454657374
301c300d06092A864886F70D0101010500030b0030080202ffff0302ffff":"":MBEDTLS_ERR_PK_INVALID_PU
BKEY + MBEDTLS_ERR_ASN1_UNEXPECTED_TAG

X509
Certificate ASN1 (TBSCertificate, pubkey, total length mismatch)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"30753073a0030201028204deadbeef300d06092a864886f70d0101020500300c310a30080600130454
657374301c170c3039303130313030303030170c3039313233313233335393539300c310a30080600130454657374
301d300d06092A864886F70D0101010500030b0030080202ffff0202ffff00":"":MBEDTLS_ERR_PK_INVALID_P
UBKEY + MBEDTLS_ERR_ASN1_LENGTH_MISMATCH

X509 Certificate ASN1 (TBSCertificate, pubkey, check failed)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"30743072a0030201028204deadbeef300d06092a864886f70d0101020500300c310a30080600130454
657374301c170c3039303130313030303030170c3039313233313233335393539300c310a30080600130454657374
301c300d06092A864886F70D0101010500030b0030080202ffff0202ffff":"":MBEDTLS_ERR_PK_INVALID_PU
BKEY

X509 Certificate ASN1 (TBSCertificate, pubkey, check failed, expanded length notation)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"308183308180a0030201028204deadbeef300d06092a864886f70d0101020500300c310a3008060013
0454657374301c170c3039303130313030303030170c3039313233313233335393539300c310a3008060013045465
7374302a300d06092A864886F70D010101050003190030160210ffffffffffffffffffffffffffffffe0202ffff":"":MBEDTL
S_ERR_PK_INVALID_PUBKEY

X509
Certificate ASN1 (TBSCertificate v3, Optional UIDs, Extensions not present)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"308183308180a0030201028204deadbeef300d06092a864886f70d0101020500300c310a3008060013
0454657374301c170c3039303130313030303030170c3039313233313233335393539300c310a3008060013045465
7374302a300d06092A864886F70D010101050003190030160210ffffffffffffffffffffffffffffffff0202ffff":"":MBEDTL
S_ERR_X509_INVALID_ALG + MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 Certificate ASN1 (TBSCertificate v3, issuerID wrong tag)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"308184308181a0030201028204deadbeef300d06092a864886f70d0101020500300c310a3008060013
0454657374301c170c3039303130313030303030170c3039313233313233335393539300c310a3008060013045465
7374302a300d06092A864886F70D010101050003190030160210ffffffffffffffffffffffffffffffff0202ffff00":"":MBEDT
LS_ERR_X509_INVALID_FORMAT
+ MBEDTLS_ERR_ASN1_LENGTH_MISMATCH

X509 Certificate ASN1 (TBSCertificate v3, UIDs, no ext)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"308189308186a0030201028204deadbeef300d06092a864886f70d0101020500300c310a3008060013
0454657374301c170c3039303130313030303030170c3039313233313233335393539300c310a3008060013045465

7374302a300d06092A864886F70D0101010500031900301602l0ffffffffffffffffffffffffffffff0202ffffa101aaa201bb"
:"":MBEDTLS_ERR_X509_INVALID_ALG + MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 Certificate ASN1 (TBSCertificate v3, UIDs, invalid length)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"308189308186a0030201028204deadbeef300d06092a864886f70d0101020500300c310a3008060013
0454657374301c170c303930313031303030303030170c303931323331323335393539300c310a3008060013045465
7374302a300d06092A864886F70D0101010500031900301602l0ffffffffffffffffffffffffffffff0202ffffa185aaa201bb"
:"":MBEDTLS_ERR_ASN1_INVALID_LENGTH

X509
Certificate ASN1 (TBSCertificate v3, ext empty)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"30818b308188a0030201028204deadbeef300d06092a864886f70d0101020500300c310a3008060013
0454657374301c170c303930313031303030303030170c303931323331323335393539300c310a3008060013045465
7374302a300d06092A864886F70D0101010500031900301602l0ffffffffffffffffffffffffffffff0202ffffa101aaa201bba
300":"":MBEDTLS_ERR_X509_INVALID_EXTENSIONS + MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 Certificate ASN1 (TBSCertificate v3, ext length mismatch)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"30818e30818ba0030201028204deadbeef300d06092a864886f70d0101020500300c310a3008060013
0454657374301c170c303930313031303030303030170c303931323331323335393539300c310a3008060013045465
7374302a300d06092A864886F70D0101010500031900301602l0ffffffffffffffffffffffffffffff0202ffffa101aaa201bba
303300000":"":MBEDTLS_ERR_X509_INVALID_EXTENSIONS +
MBEDTLS_ERR_ASN1_LENGTH_MISMATCH

X509
Certificate ASN1 (TBSCertificate v3, first ext invalid)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"30818f30818ca0030201028204deadbeef300d06092a864886f70d0101020500300c310a3008060013
0454657374301c170c303930313031303030303030170c303931323331323335393539300c310a3008060013045465
7374302a300d06092A864886F70D0101010500031900301602l0ffffffffffffffffffffffffffffff0202ffffa101aaa201bba
30330023000":"":MBEDTLS_ERR_X509_INVALID_EXTENSIONS +
MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 Certificate ASN1 (TBSCertificate v3, first ext invalid tag)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"30819030818da0030201028204deadbeef300d06092a864886f70d0101020500300c310a3008060013
0454657374301c170c303930313031303030303030170c303931323331323335393539300c310a3008060013045465
7374302a300d06092A864886F70D0101010500031900301602l0ffffffffffffffffffffffffffffff0202ffffa101aaa201bba
3043002310000":"":MBEDTLS_ERR_X509_INVALID_EXTENSIONS +
MBEDTLS_ERR_ASN1_UNEXPECTED_TAG

X509
Certificate ASN1 (TBSCertificate v3, ext BasicContraint tag, bool len missing)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"308198308195a0030201028204deadbeef300d06092a864886f70d0101020500300c310a3008060013
0454657374301c170c303930313031303030303030170c303931323331323335393539300c310a3008060013045465

7374302a300d06092A864886F70D0101010500031900301602 10ffffffffffffffffffffffffffffff0202ffffa101aaa201bba
30c300a30060603551d1301010100":"":MBEDTLS_ERR_X509_INVALID_EXTENSIONS +
MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 Certificate ASN1 (TBSCertificate v3, ext BasicContraint tag, data missing)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"308198308195a0030201028204deadbeef300d06092a864886f70d0101020500300c310a3008060013
0454657374301c170c303930313031303030303030170c303931323331323335393539300c310a3008060013045465
7374302a300d06092A864886F70D0101010500031900301602 10ffffffffffffffffffffffffffffff0202ffffa101aaa201bba
30c300a30080603551d1301010100":"":MBEDTLS_ERR_X509_INVALID_EXTENSIONS
+ MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 Certificate ASN1 (TBSCertificate v3, ext BasicContraint tag, no octet present)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"308198308195a0030201028204deadbeef300d06092a864886f70d0101020500300c310a3008060013
0454657374301c170c303930313031303030303030170c303931323331323335393539300c310a3008060013045465
7374302a300d06092A864886F70D0101010500031900301602 10ffffffffffffffffffffffffffffff0202ffffa101aaa201bba
30d300b30090603551d1301010100":"":MBEDTLS_ERR_X509_INVALID_EXTENSIONS +
MBEDTLS_ERR_ASN1_UNEXPECTED_TAG

X509 Certificate ASN1 (TBSCertificate v3, ext BasicContraint tag, octet data missing)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"30819c308199a0030201028204deadbeef300d06092a864886f70d0101020500300c310a3008060013
0454657374301c170c303930313031303030303030170c303931323331323335393539300c310a3008060013045465
7374302a300d06092A864886F70D0101010500031900301602 10ffffffffffffffffffffffffffffff0202ffffa101aaa201bba
311300f300d0603551d130101010403300100":"":MBEDTLS_ERR_X509_INVALID_EXTENSIONS
+ MBEDTLS_ERR_ASN1_UNEXPECTED_TAG

X509 Certificate ASN1 (TBSCertificate v3, ext BasicContraint tag, no pathlen)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"30819f30819ca0030201028204deadbeef300d06092a864886f70d0101020500300c310a3008060013
0454657374301c170c303930313031303030303030170c303931323331323335393539300c310a3008060013045465
7374302a300d06092A864886F70D0101010500031900301602 10ffffffffffffffffffffffffffffff0202ffffa101aaa201bba
314301230100603551d130101010406300402010102":"":MBEDTLS_ERR_X509_INVALID_EXTENSIONS +
MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 Certificate ASN1 (TBSCertificate v3, ext BasicContraint tag, octet len mismatch)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"3081a230819fa0030201028204deadbeef300d06092a864886f70d0101020500300c310a3008060013
0454657374301c170c303930313031303030303030170c303931323331323335393539300c310a3008060013045465
7374302a300d06092A864886F70D0101010500031900301602 10ffffffffffffffffffffffffffffff0202ffffa101aaa201bba
317301530130603551d13010101040930070201010201010 0":"":MBEDTLS_ERR_X509_INVALID_EXTENSIO
NS
+ MBEDTLS_ERR_ASN1_LENGTH_MISMATCH

X509 Certificate ASN1 (ExtKeyUsage, bad second tag)
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA1_C
x509parse_crt:"3081de3081dba003020102020900ebdbcd14105e1839300906072a8648ce3d0401300f310d300b0603

55040313045465737430 1e170d313431313131323035393534 5a170d323431313038323035393534 5a300f310d300b06035504031304546573743059301306072a8648ce3d020106082a8648ce3d0301070342000437cc56d976091e5a723ec7592dff206eee7cf9069174d0ad14b5f768225962924ee500d82311ffea2fd2345d5d16bd8a88c26b770d55cd8a2a0efa01c8b4edffa321301f301d0603551d250416301406082b06010505070301070 82b06010505070302":"":MBEDTLS_ERR_X509_INVALID_EXTENSIONS + MBEDTLS_ERR_ASN1_UNEXPECTED_TAG

X509 Certificate ASN1 (SubjectAltName repeated)
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA1_C
x509parse_crt:"3081fd3081faa003020102020900a8b31ff37d09a37f300906072a8648ce3d0401300f310d300b0603550403130454657374301e170d313431313131323133373136 5a170d323431313038323133373136 5a300f310d300b0603550403130454657374305930130 6072a8648ce3d020106082a8648ce3d0301070342000437cc56d976091e5a723ec7592dff206eee7cf9069174d0ad14b5f768225962924ee500d82311ffea2fd2345d5d16bd8a88c26b770d55cd8a2a0efa01c8b4edffa321301f301d0603551d11041630148208666f6f2e746573748 2086261722e74657374301d0603551d11041630148208666f6f2e746573748 2086261722e74657374":"":MBEDTLS_ERR_X509_INVALID_EXTENSIONS

X509
Certificate ASN1 (ExtKeyUsage repeated)
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA1_C
x509parse_crt:"3081fd3081faa003020102020900ebdbcd14105e1839300906072a8648ce3d0401300f310d300b0603550403130454657374301e170d313431313131323035393534 5a170d323431313038323035393534 5a300f310d300b0603550403130454657374305930130 6072a8648ce3d020106082a8648ce3d0301070342000437cc56d976091e5a723ec7592dff206eee7cf9069174d0ad14b5f768225962924ee500d82311ffea2fd2345d5d16bd8a88c26b770d55cd8a2a0efa01c8b4edffa340303e301d0603551d250416301406082b06010505070301061 82b06010505070302301d0603551d250416301406082b06010505070301061 82b06010505070302":"":MBEDTLS_ERR_X509_INVALID_EXTENSIONS

X509
Certificate ASN1 (correct pubkey, no sig_alg)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"308183308180a0030201008204deadbeef300d06092a864886f70d0101020500300c310a3008060013045465737430 1c170c3039303130313030303030 30170c3039313233313233353935393 00c310a3008060013045465737430 2a300d06092A864886F70D0101010500031900301602 10ffffffffffffffffffffffffffffffffffffffff0202ffff":"":MBEDTLS_ERR_X509_INVALID_ALG + MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 Certificate ASN1 (sig_alg mismatch)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"308192308180a0030201008204deadbeef300d06092a864886f70d0101020500300c310a3008060013045465737430 1c170c3039303130313030303030 30170c3039313233313233353935393 00c310a3008060013045465737430 2a300d06092A864886F70D0101010500031900301602 10ffffffffffffffffffffffffffffffffffffffff0202ffff300d06092a864886f70d0102020500":"":MBEDTLS_ERR_X509_SIG_MISMATCH

X509
Certificate ASN1 (sig_alg, no sig)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"308192308180a0030201008204deadbeef300d06092a864886f70d0101020500300c310a3008060013045465737430 1c170c3039303130313030303030 30170c3039313233313233353935393 00c310a3008060013045465737430 2a300d06092A864886F70D0101010500031900301602 10ffffffffffffffffffffffffffffffffffffffff0202ffff300d06092a864886f70d0101020500":"":MBEDTLS_ERR_X509_INVALID_SIGNATURE +

MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 Certificate ASN1 (signature, invalid sig data)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"308195308180a0030201008204deadbeef300d06092a864886f70d0101020500300c310a3008060013
0454657374301c170c303930313031303030303030170c303931323331323335393539300c310a3008060013045465
7374302a300d06092A864886F70D010101050003190030160210ffffffffffffffffffffffffffffff0202ffff300d06092a86
4886f70d0101020500030100":"":MBEDTLS_ERR_X509_INVALID_SIGNATURE +
MBEDTLS_ERR_ASN1_INVALID_DATA

X509
Certificate ASN1 (signature, data left)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"308197308180a0030201008204deadbeef300d06092a864886f70d0101020500300c310a3008060013
0454657374301c170c303930313031303030303030170c303931323331323335393539300c310a3008060013045465
7374302a300d06092A864886F70D010101050003190030160210ffffffffffffffffffffffffffffff0202ffff300d06092a86
4886f70d0101020500030200ff00":"":MBEDTLS_ERR_X509_INVALID_FORMAT +
MBEDTLS_ERR_ASN1_LENGTH_MISMATCH

X509 Certificate ASN1 (correct)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"308196308180a0030201008204deadbeef300d06092a864886f70d0101020500300c310a3008060013
0454657374301c170c303930313031303030303030170c303931323331323335393539300c310a3008060013045465
7374302a300d06092A864886F70D010101050003190030160210ffffffffffffffffffffffffffffff0202ffff300d06092a86
4886f70d0101020500030200ff":"cert. version \: 1\nserial number \: DE\:AD\:BE\:EF\nissuer name \:
?\?=Test\nsubject
name \: ?\?=Test\nissued on \: 2009-01-01 00\:00\:00\nexpires on \: 2009-12-31 23\:59\:59\nsigned
using \: RSA with MD2\nRSA key size \: 128 bits\n":0

X509 Certificate ASN1 (GeneralizedTime instead of UTCTime)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"308198308182a0030201008204deadbeef300d06092a864886f70d0101020500300c310a3008060013
0454657374301e180e323031303031303130303030303030170c303931323331323335393539300c310a300806001304
54657374302a300d06092A864886F70D010101050003190030160210ffffffffffffffffffffffffffffff0202ffff300d0609
2a864886f70d0101020500030200ff":"cert. version \: 1\nserial number \: DE\:AD\:BE\:EF\nissuer name \:
?\?=Test\nsubject name \: ?\?=Test\nissued on \: 2010-01-01 00\:00\:00\nexpires on \: 2009-12-31
23\:59\:59\nsigned using \: RSA with MD2\nRSA key size \: 128 bits\n":0

X509 Certificate ASN1 (Name with X520 CN)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"308199308183a0030201008204deadbeef300d06092a864886f70d0101020500300f310d300b060355
040313045465737430 1c170c303930313031303030303030170c303931323331323335393539300c310a3008060013
0454657374302a300d06092A864886F70D010101050003190030160210ffffffffffffffffffffffffffffff0202ffff300d06
092a864886f70d0101020500030200ff":"cert.
version \: 1\nserial number \: DE\:AD\:BE\:EF\nissuer name \: CN=Test\nsubject name \:
?\?=Test\nissued on \: 2009-01-01 00\:00\:00\nexpires on \: 2009-12-31 23\:59\:59\nsigned using \:
RSA with MD2\nRSA key size \: 128 bits\n":0

X509 Certificate ASN1 (Name with X520 C)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"308199308183a0030201008204deadbeef300d06092a864886f70d0101020500300f310d300b060355
040613045465737430 1c170c3039303130313030303030 30170c3039313233313233353935393030 1c310a3008060013
0454657374302a300d06092A864886F70D0101010500031900301602 10ffffffffffffffffffffffffffffff0202ffff300d06
092a864886f70d0101020500030200ff":"cert.
version \: 1\nserial number \: DE\:AD\:BE\:EF\nissuer name \: C=Test\nsubject name \:
?\?=Test\nissued on \: 2009-01-01 00\:00\:00\nexpires on \: 2009-12-31 23\:59\:59\nsigned using \:
RSA with MD2\nRSA key size \: 128 bits\n":0

X509 Certificate ASN1 (Name with X520 L)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"308199308183a0030201008204deadbeef300d06092a864886f70d0101020500300f310d300b060355
040713045465737430 1c170c3039303130313030303030 30170c3039313233313233353935393030 1c310a3008060013
0454657374302a300d06092A864886F70D0101010500031900301602 10ffffffffffffffffffffffffffffff0202ffff300d06
092a864886f70d0101020500030200ff":"cert. version \: 1\nserial number \: DE\:AD\:BE\:EF\nissuer name
\: L=Test\nsubject name \: ?\?=Test\nissued on \: 2009-01-01 00\:00\:00\nexpires on \: 2009-12-31
23\:59\:59\nsigned using \: RSA with MD2\nRSA key size \: 128 bits\n":0

X509 Certificate ASN1 (Name with X520
ST)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"308199308183a0030201008204deadbeef300d06092a864886f70d0101020500300f310d300b060355
040813045465737430 1c170c3039303130313030303030 30170c3039313233313233353935393030 1c310a3008060013
0454657374302a300d06092A864886F70D0101010500031900301602 10ffffffffffffffffffffffffffffff0202ffff300d06
092a864886f70d0101020500030200ff":"cert. version \: 1\nserial number \: DE\:AD\:BE\:EF\nissuer name
\: ST=Test\nsubject name \: ?\?=Test\nissued on \: 2009-01-01 00\:00\:00\nexpires on \: 2009-12-31
23\:59\:59\nsigned using \: RSA with MD2\nRSA key size \: 128 bits\n":0

X509 Certificate ASN1 (Name with X520 O)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"308199308183a0030201008204deadbeef300d06092a864886f70d0101020500300f310d300b060355
040a13045465737430 1c170c3039303130313030303030 30170c3039313233313233353935393030 1c310a3008060013
0454657374302a300d06092A864886F70D0101010500031900301602 10ffffffffffffffffffffffffffffff0202ffff300d06
092a864886f70d0101020500030200ff":"cert.
version \: 1\nserial number \: DE\:AD\:BE\:EF\nissuer name \: O=Test\nsubject name \:
?\?=Test\nissued on \: 2009-01-01 00\:00\:00\nexpires on \: 2009-12-31 23\:59\:59\nsigned using \:
RSA with MD2\nRSA key size \: 128 bits\n":0

X509 Certificate ASN1 (Name with X520 OU)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"308199308183a0030201008204deadbeef300d06092a864886f70d0101020500300f310d300b060355
040b13045465737430 1c170c3039303130313030303030 30170c3039313233313233353935393030 1c310a3008060013
0454657374302a300d06092A864886F70D0101010500031900301602 10ffffffffffffffffffffffffffffff0202ffff300d06
092a864886f70d0101020500030200ff":"cert. version \: 1\nserial number \: DE\:AD\:BE\:EF\nissuer name
\: OU=Test\nsubject name \: ?\?=Test\nissued on \: 2009-01-01 00\:00\:00\nexpires on \: 2009-12-31
23\:59\:59\nsigned using \: RSA with MD2\nRSA

key size \: 128 bits\n":0

X509 Certificate ASN1 (Name with unknown X520 part)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"308199308183a0030201008204deadbeef300d06092a864886f70d0101020500300f310d300b060355
04de130454657374301c170c303930313031303030303030170c303931323331323335393539300c310a3008060013
0454657374302a300d06092A864886F70D0101010500031900301602 10ffffffffffffffffffffffffffffffffffff0202ffff300d06
092a864886f70d0101020500030200ff":"cert. version \: 1\nserial number \: DE\:AD\:BE\:EF\nissuer name
\: ?\?=Test\nsubject name \: ?\?=Test\nissued on \: 2009-01-01 00\:00\:00\nexpires on \: 2009-12-31
23\:59\:59\nsigned using \: RSA with MD2\nRSA key size \: 128 bits\n":0

X509 Certificate ASN1 (Name with composite RDN)
depends_on:MBEDTLS_RSA_C:MBEDTLS_SHA1_C
x509parse_crt:"3082029f30820208a00302010202044c20e3bd300d06092a864886f70d0101050500305631 0b300906
0355040613025553310b300906035504080c0243413121301f060355040a0c18496e7465726e657420576964676974
7320507479204c7464311730150603550403 0c0e4672616e6b656e63657274204341301e170d313330383032313531
3433375a170d3135303831373035353433315a3081d1310b3009060355040613025553311330110603550408130a5
7617368696e67746f6e31133011060b2b0601040182373c020103130255533119301706 0b2b0601040182373c02010
2130844656c6177617265311a3018060355040a1311417574686f72697a652e4e6574204c4c43311d301b060355040f
131450726976617465204f7267616e697a6174696f6e312a300e060355040513073433363931393130180603550403
13117777772e617574686f72697a652e6e6574311630140603550407130d53616e204672616e636973636f30819f300
d06092a864886f70d010101050003818d0030818902818100d885c62e209b6ac005c64f0bcfdaac1f2b67a18802f75b0
8851ff933deed888b7b68a62fcabdb21d4a8914becfeaaa1b7e08a09ffaf9916563586dc95e2877262b0b5f5ec27eb4d75
4aa6facd1d39d25b38a2372891bacdd3e919f791ed25704e8920e380e5623a38e6a23935978a3aec7a8e761e211d42eff
a2713e44e7de0b0203010001300d06092a864886f70d0101050500038181 00092f7424d3f6da4b8553829d958ed1980
b9270b42c0d3d5833509a28c66bb207df9f3c51d122065e00b87c08c2730d2745fe1c279d16fae4d53b4bf5bdfa3631fc
eeb2e772b6b08a3eca5a2e2c687aefd23b4b73bf77ac6099711342cf070b35c6f61333a7cbf613d8dd4bd73e9df34bcd4
284b0b4df57c36c450613f11e5dac":"cert.
version \: 3\nserial number \: 4C\:20\:E3\:BD\nissuer name \: C=US, ST=CA, O=Internet Widgits Pty Ltd,
CN=Frankencert CA\nsubject name \: C=US, ST=Washington, ??=US, ??=Delaware, O=Authorize.Net LLC,
??=Private Organization, serialNumber=4369191 + CN=www.authorize.net, L=San Francisco\nissued on \:
2013-08-02 15\:14\:37\nexpires on \: 2015-08-17 05\:54\:31\nsigned using \: RSA with SHA1\nRSA key
size \: 1024 bits\n":0

X509 Certificate ASN1 (Name with PKCS9 email)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"30819f308189a0030201008204deadbeef300d06092a864886f70d0101020500301531133011060 92a
864886f70d0109011304546573743 01c170c303930313031303030303030170c303931323331323335393539300c31
0a3008060013045465737430 2a300d06092A864886F70D0101010500031900301602 10ffffffffffffffffffffffffffffffffffff0
202ffff300d06092a864886f70d0101020500030200ff":"cert.
version \: 1\nserial number \: DE\:AD\:BE\:EF\nissuer name \: emailAddress=Test\nsubject name \:
?\?=Test\nissued on \: 2009-01-01 00\:00\:00\nexpires on \: 2009-12-31 23\:59\:59\nsigned using \:
RSA with MD2\nRSA key size \: 128 bits\n":0

X509 Certificate ASN1 (Name with unknown PKCS9 part)
depends_on:MBEDTLS_RSA_C:MBEDTLS_MD2_C
x509parse_crt:"30819f308189a0030201008204deadbeef300d06092a864886f70d0101020500301531133011060 92a
864886f70d0109ab130454657374301c170c303930313031303030303030170c303931323331323335393539300c31

0a3008060013045465737430 2a300d06092A864886F70D01010105000319003016021 0fffffffffffffffffffffffffffffff0
202ffff300d06092a864886f70d0101020500030200ff":"cert. version \: 1\nserial number \:
DE\:AD\:BE\:EF\nissuer name \: ?\?=Test\nsubject name \: ?\?=Test\nissued on \: 2009-01-01
00\:00\:00\nexpires on
\: 2009-12-31 23\:59\:59\nsigned using \: RSA with MD2\nRSA key size \: 128 bits\n":0

X509 Certificate ASN1 (ECDSA signature, RSA key)
depends_on:MBEDTLS_RSA_C:MBEDTLS_SHA1_C:MBEDTLS_ECDSA_C
x509parse_crt:"3081E630819E020103300906072A8648CE3D0401300F310D300B060355040313045465737430 1
E170D313330373130303943631385A170D323330373038303943631385A300F310D300B06035504031304546
57374304C300D06092A864886F70D0101010500033B003038023100E8F546061D3B49BC2F6B7524B7EA4D73
A8D5293EE8C64D9407B70B5D16BAEBC32B8205591EAB4E1EB57E92418837012502030100013009060 72A8
648CE3D040103380030350218 6E18209AFBED14A0D9A796EFCAD68891E3CCD5F75815C833021900E92B4F
D460B1994693243B9FFAD54729DE865381BDA41D25":"cert. version \: 1\nserial number \: 03\nissuer name
\: CN=Test\nsubject name \: CN=Test\nissued on \: 2013-07-10 09\:46\:18\nexpires on \: 2023-07-08
09\:46\:18\nsigned using \: ECDSA with SHA1\nRSA key size \: 384 bits\n":0

X509 Certificate ASN1 (ECDSA signature,
EC key)
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP192R1_ENABLED:MBEDTLS_SHA1_C
x509parse_crt:"3081EB3081A3020900F41534662EC7E912300906072A8648CE3D0401300F310D300B06035504
03130454657374301E170D313330373130303943031395A170D323330373038303943031395A300F310D300B
060355040313045465737430493013060 72A8648CE3D020106082A8648CE3D030101033200042137969FABD4E
370624A0E1A33E379CAB950CCE00EF8C3C3E2ADAEB7271C8F07659D65D3D777DCF21614363AE4B6E617
300906072A8648CE3D040103380030350218 58CC0F957946FE6A303D92885A456AA74C743C7B708CBD3702
1900FE293CAC21AF352D16B82EB8EA54E9410B3ABAADD9F05DD6":"cert. version \: 1\nserial number \:
F4\:15\:34\:66\:2E\:C7\:E9\:12\nissuer name \: CN=Test\nsubject name \: CN=Test\nissued on \: 2013-
07-10 09\:40\:19\nexpires on \: 2023-07-08 09\:40\:19\nsigned using \: ECDSA with SHA1\nEC key size
\: 192 bits\n":0

X509 Certificate ASN1 (RSA signature, EC key)
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP192R1_ENABLED:MBEDTLS_SHA1_C
x509parse_crt:"3081E430819F020104300D06092A864886F70D0101050500300F310D300B060355040313045465
7374301E170D313330373130313530323337 5A170D323330373038313530323337 5A300F310D300B0603550403
130454657374304930130 6072A8648CE3D020106082A8648CE3D030101033200 4E962551A325B21B50CF6B9
90E33D4318FD16677130726357A196E3EFE7107BCB6BDC6D9DB2A4DF7C964ACFE81798433D300D06092A
864886F70D0101050500033100 1A6C18CD1E457474B2D3912743F44B571341A7859A0122774A8E19A6716808
78936949F904C9255BDD6FFFDB33A7E6D8":"cert.
version \: 1\nserial number \: 04\nissuer name \: CN=Test\nsubject name \: CN=Test\nissued on \:
2013-07-10 15\:02\:37\nexpires on \: 2023-07-08 15\:02\:37\nsigned using \: RSA with SHA1\nEC key size
\: 192 bits\n":0

X509 Certificate ASN1 (invalid version 3)
x509parse_crt:"30173015a0030201038204deadbeef30080604cafed00d0500":"":MBEDTLS_ERR_X509_UNKNO
WN_VERSION

X509 Certificate ASN1 (invalid version overflow)
x509parse_crt:"301A3018a00602047FFFFFFF8204deadbeef30080604cafed00d0500":"":MBEDTLS_ERR_X509_

UNKNOWN_VERSION

X509
CRL ASN1 (Incorrect first tag)
x509parse_crl:"":"":MBEDTLS_ERR_X509_INVALID_FORMAT

X509 CRL ASN1 (Correct first tag, data length does not match)
x509parse_crl:"300000":"":MBEDTLS_ERR_X509_INVALID_FORMAT +
MBEDTLS_ERR_ASN1_LENGTH_MISMATCH

X509 CRL ASN1 (TBSCertList, tag missing)
x509parse_crl:"3000":"":MBEDTLS_ERR_X509_INVALID_FORMAT +
MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 CRL ASN1 (TBSCertList, version tag len missing)
x509parse_crl:"3003300102":"":MBEDTLS_ERR_X509_INVALID_VERSION +
MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 CRL ASN1 (TBSCertList, version correct, alg missing)
x509parse_crl:"30053003020100":"":MBEDTLS_ERR_X509_INVALID_ALG +
MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 CRL ASN1 (TBSCertList, alg correct, incorrect version)
x509parse_crl:"300b300902010230040600050 0":"":MBEDTLS_ERR_X509_UNKNOWN_VERSION

X509 CRL ASN1 (TBSCertList, correct version, sig_oid1 unknown)
x509parse_crl:"300b300902010030040600050 0":"":MBEDTLS_ERR_X509_UNKNOWN_SIG_ALG

X509
CRL ASN1 (TBSCertList, sig_oid1 id unknown)
x509parse_crl:"30143012020100300d06092a864886f70d01010f0500":"":MBEDTLS_ERR_X509_UNKNOWN_SI
G_ALG

X509 CRL ASN1 (TBSCertList, sig_oid1 correct, issuer missing)
depends_on:MBEDTLS_RSA_C:MBEDTLS_SHA256_C
x509parse_crl:"30143012020100300d06092a864886f70d01010e0500":"":MBEDTLS_ERR_X509_INVALID_FOR
MAT + MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 CRL ASN1 (TBSCertList, issuer set missing)
depends_on:MBEDTLS_RSA_C:MBEDTLS_SHA256_C
x509parse_crl:"30163014020100300d06092a864886f70d01010e05003000":"":MBEDTLS_ERR_X509_INVALID
_NAME + MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 CRL ASN1 (TBSCertList, correct issuer, thisUpdate missing)
depends_on:MBEDTLS_RSA_C:MBEDTLS_SHA256_C
x509parse_crl:"302530230201003 00d06092a864886f70d01010e0500300f310d300b060355040313044142434 4":"":
MBEDTLS_ERR_X509_INVALID_DATE + MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 CRL ASN1 (TBSCertList, correct thisUpdate, nextUpdate missing, entries length missing)
depends_on:MBEDTLS_RSA_C:MBEDTLS_SHA256_C
x509parse_crl:"30343032020100300d06092a864886f70d01010e0500300f310d300b06035504031304414243441704
c303930313031303030303030":"":MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509
CRL ASN1 (TBSCertList, entries present, invalid sig_alg)
depends_on:MBEDTLS_RSA_C:MBEDTLS_SHA256_C
x509parse_crl:"304a3047020100300d06092a864886f70d01010e0500300f310d300b06035504031304414243441704c
303930313031303030303030301430128202abcd170c303831323331323335393539003":"":MBEDTLS_ERR_X509
_INVALID_ALG + MBEDTLS_ERR_ASN1_UNEXPECTED_TAG

X509 CRL ASN1 (TBSCertList, entries present, date in entry invalid)
depends_on:MBEDTLS_RSA_C:MBEDTLS_SHA256_C
x509parse_crl:"304a3047020100300d06092a864886f70d01010e0500300f310d300b06035504031304414243441704c
303930313031303030303030301430128202abcd190c303831323331323335393539003":"":MBEDTLS_ERR_X509
_INVALID_DATE + MBEDTLS_ERR_ASN1_UNEXPECTED_TAG

X509 CRL ASN1 (TBSCertList, sig_alg present, sig_alg does not match)
depends_on:MBEDTLS_RSA_C:MBEDTLS_SHA256_C
x509parse_crl:"30583047020100300d06092a864886f70d01010e0500300f310d300b06035504031304414243441704
c303930313031303030303030301430128202abcd170c303831323331323335393539300d06092a864886f70d01010
d0500":"":MBEDTLS_ERR_X509_SIG_MISMATCH

X509
CRL ASN1 (TBSCertList, sig present, len mismatch)
depends_on:MBEDTLS_RSA_C:MBEDTLS_SHA256_C
x509parse_crl:"305d3047020100300d06092a864886f70d01010e0500300f310d300b06035504031304414243441704
c303930313031303030303030301430128202abcd170c303831323331323335393539300d06092a864886f70d01010
e05000302000100":"":MBEDTLS_ERR_X509_INVALID_FORMAT +
MBEDTLS_ERR_ASN1_LENGTH_MISMATCH

X509 CRL ASN1 (TBSCertList, sig present)
depends_on:MBEDTLS_RSA_C:MBEDTLS_SHA256_C
x509parse_crl:"305c3047020100300d06092a864886f70d01010e0500300f310d300b06035504031304414243441704c
303930313031303030303030301430128202abcd170c303831323331323335393539300d06092a864886f70d01010e
050003020001":"CRL version \: 1\nissuer name \: CN=ABCD\nthis update \: 2009-01-01 00\:00\:00\nnext
update \: 0000-00-00 00\:00\:00\nRevoked certificates\:\nserial
number\: AB\:CD revocation date\: 2008-12-31 23\:59\:59\nsigned using \: RSA with SHA-224\n":0

X509 CRL ASN1 (TBSCertList, no entries)
depends_on:MBEDTLS_RSA_C:MBEDTLS_SHA256_C
x509parse_crl:"30463031020100300d06092a864886f70d01010e0500300f310d300b06035504031304414243441704
c303930313031303030303030300d06092a864886f70d01010e050003020001":"CRL version \: 1\nissuer name \:
CN=ABCD\nthis update \: 2009-01-01 00\:00\:00\nnext update \: 0000-00-00 00\:00\:00\nRevoked
certificates\:\nsigned using \: RSA with SHA-224\n":0

X509 CRL ASN1 (invalid version 2)

x509parse_crl:"30463031020102300d06092a864886f70d01010e0500300f310d300b06035504031304414243441700
c303930313031303030303030300d06092a864886f70d01010e050003020001":"":MBEDTLS_ERR_X509_UNKN
OWN_VERSION

X509 CRL ASN1 (invalid version overflow)
x509parse_crl:"3049303102047FFFFFFF300d06092a864886f70d01010e0500300f310d300b0603550403130441424
344170c303930313031303030303030300d06092a864886f70d01010e050003020001":"":MBEDTLS_ERR_X509_
UNKNOWN_VERSION

X509
CRT parse path #2 (one cert)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_RSA_C
mbedtls_x509_crt_parse_path:"data_files/dir1":0:1

X509 CRT parse path #3 (two certs)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_SHA256_C:MBEDTLS_ECDSA_C:MBEDT
LS_ECP_DP_SECP384R1_ENABLED
mbedtls_x509_crt_parse_path:"data_files/dir2":0:2

X509 CRT parse path #4 (two certs, one non-cert)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_SHA256_C:MBEDTLS_ECDSA_C:MBEDT
LS_ECP_DP_SECP384R1_ENABLED
mbedtls_x509_crt_parse_path:"data_files/dir3":1:2

X509 CRT verify long chain (max intermediate CA, trusted)
depends_on:MBEDTLS_SHA256_C:MBEDTLS_ECDSA_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED
mbedtls_x509_crt_verify_max:"data_files/dir-maxpath/00.crt":"data_files/dir-
maxpath":MBEDTLS_X509_MAX_INTERMEDIATE_CA:0:0

X509 CRT verify long chain (max intermediate CA, untrusted)
depends_on:MBEDTLS_SHA256_C:MBEDTLS_ECDSA_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MB
EDTLS_ECP_DP_SECP384R1_ENABLED
mbedtls_x509_crt_verify_max:"data_files/test-ca2.crt":"data_files/dir-
maxpath":MBEDTLS_X509_MAX_INTERMEDIATE_CA-
1:MBEDTLS_ERR_X509_CERT_VERIFY_FAILED:MBEDTLS_X509_BADCERT_NOT_TRUSTED

X509
CRT verify long chain (max intermediate CA + 1)
depends_on:MBEDTLS_SHA256_C:MBEDTLS_ECDSA_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED
mbedtls_x509_crt_verify_max:"data_files/dir-maxpath/00.crt":"data_files/dir-
maxpath":MBEDTLS_X509_MAX_INTERMEDIATE_CA+1:MBEDTLS_ERR_X509_FATAL_ERROR:-1

X509 CRT verify chain #1 (zero pathlen intermediate)
depends_on:MBEDTLS_SHA256_C:MBEDTLS_RSA_C
mbedtls_x509_crt_verify_chain:"data_files/dir4/cert14.crt data_files/dir4/cert13.crt
data_files/dir4/cert12.crt":"data_files/dir4/cert11.crt":MBEDTLS_X509_BADCERT_NOT_TRUSTED

X509 CRT verify chain #2 (zero pathlen root)

depends_on:MBEDTLS_SHA256_C:MBEDTLS_RSA_C
mbedtls_x509_crt_verify_chain:"data_files/dir4/cert23.crt
data_files/dir4/cert22.crt":"data_files/dir4/cert21.crt":MBEDTLS_X509_BADCERT_NOT_TRUSTED

X509 CRT verify chain #3 (nonzero pathlen root)
depends_on:MBEDTLS_SHA256_C:MBEDTLS_RSA_C
mbedtls_x509_crt_verify_chain:"data_files/dir4/cert34.crt
data_files/dir4/cert33.crt
data_files/dir4/cert32.crt":"data_files/dir4/cert31.crt":MBEDTLS_X509_BADCERT_NOT_TRUSTED

X509 CRT verify chain #4 (nonzero pathlen intermediate)
depends_on:MBEDTLS_SHA256_C:MBEDTLS_RSA_C
mbedtls_x509_crt_verify_chain:"data_files/dir4/cert45.crt data_files/dir4/cert44.crt data_files/dir4/cert43.crt
data_files/dir4/cert42.crt":"data_files/dir4/cert41.crt":MBEDTLS_X509_BADCERT_NOT_TRUSTED

X509 CRT verify chain #5 (nonzero maxpathlen intermediate)
depends_on:MBEDTLS_SHA256_C:MBEDTLS_RSA_C
mbedtls_x509_crt_verify_chain:"data_files/dir4/cert54.crt data_files/dir4/cert53.crt
data_files/dir4/cert52.crt":"data_files/dir4/cert51.crt":0

X509 CRT verify chain #6 (nonzero maxpathlen root)
depends_on:MBEDTLS_SHA256_C:MBEDTLS_RSA_C
mbedtls_x509_crt_verify_chain:"data_files/dir4/cert63.crt data_files/dir4/cert62.crt":"data_files/dir4/cert61.crt":0

X509 CRT verify chain #7 (maxpathlen
root, self signed in path)
depends_on:MBEDTLS_SHA256_C:MBEDTLS_RSA_C
mbedtls_x509_crt_verify_chain:"data_files/dir4/cert74.crt data_files/dir4/cert73.crt
data_files/dir4/cert72.crt":"data_files/dir4/cert71.crt":0

X509 CRT verify chain #8 (self signed maxpathlen root)
depends_on:MBEDTLS_SHA256_C:MBEDTLS_RSA_C
mbedtls_x509_crt_verify_chain:"data_files/dir4/cert61.crt data_files/dir4/cert63.crt
data_files/dir4/cert62.crt":"data_files/dir4/cert61.crt":0

X509 CRT verify chain #9 (zero pathlen first intermediate, valid)
depends_on:MBEDTLS_SHA256_C:MBEDTLS_ECDSA_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED
mbedtls_x509_crt_verify_chain:"data_files/dir4/cert83.crt data_files/dir4/cert82.crt":"data_files/dir4/cert81.crt":0

X509 CRT verify chain #10 (zero pathlen root, valid)
depends_on:MBEDTLS_SHA256_C:MBEDTLS_ECDSA_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED
mbedtls_x509_crt_verify_chain:"data_files/dir4/cert92.crt":"data_files/dir4/cert91.crt":0

X509 OID description #1
x509_oid_desc:"2B06010505070301":"TLS
Web Server Authentication"

X509 OID description #2

x509_oid_desc:"2B0601050507030f":"notfound"

X509 OID description #3
x509_oid_desc:"2B0601050507030100":"notfound"

X509 OID numstring #1 (wide buffer)
x509_oid_numstr:"2B06010505070301":"1.3.6.1.5.5.7.3.1":20:17

X509 OID numstring #2 (buffer just fits)
x509_oid_numstr:"2B06010505070301":"1.3.6.1.5.5.7.3.1":18:17

X509 OID numstring #3 (buffer too small)
x509_oid_numstr:"2B06010505070301":"1.3.6.1.5.5.7.3.1":17:MBEDTLS_ERR_OID_BUF_TOO_SMALL

X509 OID numstring #4 (larger number)
x509_oid_numstr:"2A864886F70D":"1.2.840.113549":15:14

X509 OID numstring #5 (arithmetic overflow)
x509_oid_numstr:"2A8648F9F8F7F6F5F4F3F2F1F001":"":100:MBEDTLS_ERR_OID_BUF_TOO_SMALL

X509 crt keyUsage #1 (no extension, expected KU)
depends_on:MBEDTLS_RSA_C:MBEDTLS_SHA1_C
x509_check_key_usage:"data_files/server1.crt":MBEDTLS_X509_KU_DIGITAL_SIGNATURE|MBEDTLS_X509_KU_KEY_ENCIPHERMENT:0

X509 crt keyUsage #2 (no extension, surprising KU)
depends_on:MBEDTLS_RSA_C:MBEDTLS_SHA1_C
x509_check_key_usage:"data_files/server1.crt":MBEDTLS_X509_KU_KEY_CERT_SIGN:0

X509
crt keyUsage #3 (extension present, no KU)
depends_on:MBEDTLS_RSA_C:MBEDTLS_SHA1_C
x509_check_key_usage:"data_files/server1.key_usage.crt":0:0

X509 crt keyUsage #4 (extension present, single KU present)
depends_on:MBEDTLS_RSA_C:MBEDTLS_SHA1_C
x509_check_key_usage:"data_files/server1.key_usage.crt":MBEDTLS_X509_KU_DIGITAL_SIGNATURE:0

X509 crt keyUsage #5 (extension present, single KU absent)
depends_on:MBEDTLS_RSA_C:MBEDTLS_SHA1_C
x509_check_key_usage:"data_files/server1.key_usage.crt":MBEDTLS_X509_KU_KEY_CERT_SIGN:MBEDTLS_ERR_X509_BAD_INPUT_DATA

X509 crt keyUsage #6 (extension present, combined KU present)
depends_on:MBEDTLS_RSA_C:MBEDTLS_SHA1_C
x509_check_key_usage:"data_files/server1.key_usage.crt":MBEDTLS_X509_KU_DIGITAL_SIGNATURE|MBEDTLS_X509_KU_KEY_ENCIPHERMENT:0

X509 crt keyUsage #7 (extension present, combined KU both absent)
depends_on:MBEDTLS_RSA_C:MBEDTLS_SHA1_C
x509_check_key_usage:"data_files/server1.key_usage.crt":MBEDTLS_X509_KU_KEY_CERT_SIGN|MBEDTLS_X509_KU_CRL_SIGN:MBEDTLS_ERR_X509_BAD_INPUT_DATA

X509
crt keyUsage #8 (extension present, combined KU one absent)
depends_on:MBEDTLS_RSA_C:MBEDTLS_SHA1_C
x509_check_key_usage:"data_files/server1.key_usage.crt":MBEDTLS_X509_KU_KEY_ENCIPHERMENT|MBEDTLS_X509_KU_KEY_AGREEMENT:MBEDTLS_ERR_X509_BAD_INPUT_DATA

X509 crt keyUsage #9 (extension present, decOnly allowed absent)
depends_on:MBEDTLS_RSA_C:MBEDTLS_SHA1_C
x509_check_key_usage:"data_files/server1.key_usage.crt":MBEDTLS_X509_KU_DIGITAL_SIGNATURE|MBEDTLS_X509_KU_KEY_ENCIPHERMENT|MBEDTLS_X509_KU_DECIPHER_ONLY:0

X509 crt keyUsage #10 (extension present, decOnly non-allowed present)
depends_on:MBEDTLS_RSA_C:MBEDTLS_SHA1_C
x509_check_key_usage:"data_files/keyUsage.decipherOnly.crt":MBEDTLS_X509_KU_DIGITAL_SIGNATURE|MBEDTLS_X509_KU_KEY_ENCIPHERMENT:MBEDTLS_ERR_X509_BAD_INPUT_DATA

X509 crt keyUsage #11 (extension present, decOnly allowed present)
depends_on:MBEDTLS_RSA_C:MBEDTLS_SHA1_C
x509_check_key_usage:"data_files/keyUsage.decipherOnly.crt":MBEDTLS_X509_KU_DIGITAL_SIGNATURE|MBEDTLS_X509_KU_KEY_ENCIPHERMENT|MBEDTLS_X509_KU_DECIPHER_ONLY:0

X509
crt extendedKeyUsage #1 (no extension, serverAuth)
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA256_C
x509_check_extended_key_usage:"data_files/server5.crt":"2B06010505070301":0

X509 crt extendedKeyUsage #2 (single value, present)
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA256_C
x509_check_extended_key_usage:"data_files/server5.eku-srv.crt":"2B06010505070301":0

X509 crt extendedKeyUsage #3 (single value, absent)
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA256_C
x509_check_extended_key_usage:"data_files/server5.eku-cli.crt":"2B06010505070301":MBEDTLS_ERR_X509_BAD_INPUT_DATA

X509 crt extendedKeyUsage #4 (two values, first)
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA256_C
x509_check_extended_key_usage:"data_files/server5.eku-srv_cli.crt":"2B06010505070301":0

X509
crt extendedKeyUsage #5 (two values, second)
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA256_C
x509_check_extended_key_usage:"data_files/server5.eku-srv_cli.crt":"2B06010505070302":0

X509 crt extendedKeyUsage #6 (two values, other)
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA256_C
x509_check_extended_key_usage:"data_files/server5.eku-
srv_cli.crt":"2B06010505070303":MBEDTLS_ERR_X509_BAD_INPUT_DATA

X509 crt extendedKeyUsage #7 (any, random)
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA256_C
x509_check_extended_key_usage:"data_files/server5.eku-cs_any.crt":"2B060105050703FF":0

X509 RSASSA-PSS parameters ASN1 (good, all defaults)
x509_parse_rsassa_pss_params:"":MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:20:0

X509 RSASSA-PSS parameters ASN1 (wrong initial tag)
x509_parse_rsassa_pss_params:"":MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA1:MBEDTLS_MD_SH
A1:20:MBEDTLS_ERR_X509_INVALID_ALG
+ MBEDTLS_ERR_ASN1_UNEXPECTED_TAG

X509 RSASSA-PSS parameters ASN1 (unknown tag in top-level sequence)
x509_parse_rsassa_pss_params:"A400":MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:20:MBEDTLS_ERR_X509_IN
VALID_ALG + MBEDTLS_ERR_ASN1_LENGTH_MISMATCH

X509 RSASSA-PSS parameters ASN1 (good, HashAlg SHA256)
depends_on:MBEDTLS_RSA_C:MBEDTLS_SHA256_C
x509_parse_rsassa_pss_params:"A00D300B06096086480165030402 01":MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA256:MBEDTLS_MD_SHA1:20:0

X509 RSASSA-PSS parameters ASN1 (good, explicit HashAlg = default)
depends_on:MBEDTLS_RSA_C:MBEDTLS_SHA1_C
x509_parse_rsassa_pss_params:"A009300706052B0E03021A":MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:20:0

X509 RSASSA-PSS parameters ASN1 (HashAlg wrong len #1)
x509_parse_rsassa_pss_params:"A00A300706052B0E03021A":MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:20:MBEDTLS_ERR_X509_IN
VALID_ALG + MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 RSASSA-PSS parameters ASN1 (HashAlg wrong len #2)
depends_on:MBEDTLS_RSA_C:MBEDTLS_SHA1_C
x509_parse_rsassa_pss_params:"A00A300706052B0E03021A00":MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:20:MBEDTLS_ERR_X509_IN
VALID_ALG + MBEDTLS_ERR_ASN1_LENGTH_MISMATCH

X509 RSASSA-PSS parameters ASN1 (HashAlg with parameters)
x509_parse_rsassa_pss_params:"A00F300D06096086480165030402013000":MBEDTLS_ASN1_CONSTRUCTE
D |

MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA256:MBEDTLS_MD_SHA1:20:MBEDTLS_ERR_X509_INVALID_ALG + MBEDTLS_ERR_ASN1_INVALID_DATA

X509 RSASSA-PSS parameters ASN1 (HashAlg unknown OID)
x509_parse_rsassa_pss_params:"A00D300B0609608648016503040 2FF":MBEDTLS_ASN1_CONSTRUCTED | MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA256:MBEDTLS_MD_SHA1:20:MBEDTLS_ERR_X509_INVALID_ALG + MBEDTLS_ERR_OID_NOT_FOUND

X509 RSASSA-PSS parameters ASN1 (good, MGAlg = MGF1-SHA256)
depends_on:MBEDTLS_RSA_C:MBEDTLS_SHA256_C
x509_parse_rsassa_pss_params:"A11A301806092A864886F70D010108300B060960864801650304020 1":MBEDTLS_ASN1_CONSTRUCTED
| MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA256:20:0

X509 RSASSA-PSS parameters ASN1 (good, explicit MGAlg = default)
depends_on:MBEDTLS_RSA_C:MBEDTLS_SHA1_C
x509_parse_rsassa_pss_params:"A116301406092A864886F70D01010830070 6052B0E03021A":MBEDTLS_ASN1_CONSTRUCTED | MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:20:0

X509 RSASSA-PSS parameters ASN1 (MGAlg wrong len #1)
x509_parse_rsassa_pss_params:"A11B301806092A864886F70D010108300B060960864801650304020 1":MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA256:20:MBEDTLS_ERR_X509_INVALID_ALG + MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 RSASSA-PSS parameters ASN1 (MGAlg wrong len #2)
depends_on:MBEDTLS_RSA_C:MBEDTLS_SHA256_C
x509_parse_rsassa_pss_params:"A11B301806092A864886F70D010108300B060960864801650304020 100":MBEDTLS_ASN1_CONSTRUCTED
|
MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA256:20:MBEDTLS_ERR_X509_INVALID_ALG + MBEDTLS_ERR_ASN1_LENGTH_MISMATCH

X509 RSASSA-PSS parameters ASN1 (MGAlg AlgId wrong len #1)
x509_parse_rsassa_pss_params:"A11A301906092A864886F70D010108300B060960864801650304020 1":MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA256:20:MBEDTLS_ERR_X509_INVALID_ALG + MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 RSASSA-PSS parameters ASN1 (MGAlg OID != MGF1)
x509_parse_rsassa_pss_params:"A11A301806092A864886F70D010109300B060960864801650304020 1":MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA256:20:MBEDTLS_ERR_X509_FEATURE_UNAVAILABLE + MBEDTLS_ERR_OID_NOT_FOUND

X509 RSASSA-PSS parameters ASN1 (MGAlg.params wrong tag)
x509_parse_rsassa_pss_params:"A11A301806092A864886F70D010108310B060960864801650304020 1":MBEDTLS_ASN1_CONSTRUCTED |

MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA256:20:MBEDTLS_ERR_X509_INVALID_ALG + MBEDTLS_ERR_ASN1_UNEXPECTED_TAG

X509
RSASSA-PSS parameters ASN1 (MGAlg.params wrong len #1a)
x509_parse_rsassa_pss_params:"A10F300D06092A864886F70D0101083000":MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA256:20:MBEDTLS_ERR_X509_INVALID_ALG + MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 RSASSA-PSS parameters ASN1 (MGAlg.params wrong len #1b)
x509_parse_rsassa_pss_params:"A11B301906092A864886F70D010108300C06096086480165030402010":MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA256:20:MBEDTLS_ERR_X509_INVALID_ALG + MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 RSASSA-PSS parameters ASN1 (MGAlg.params.alg not an OID)
x509_parse_rsassa_pss_params:"A11A301806092A864886F70D010108300B0709608648016503040201":MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA256:20:MBEDTLS_ERR_X509_INVALID_ALG + MBEDTLS_ERR_ASN1_UNEXPECTED_TAG

X509 RSASSA-PSS parameters ASN1 (MGAlg.params.alg unknown OID)
x509_parse_rsassa_pss_params:"A11A301806092A864886F70D010108300B06096086480165030402FF":MBEDTLS_ASN1_CONSTRUCTED
|
MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA256:20:MBEDTLS_ERR_X509_INVALID_ALG + MBEDTLS_ERR_OID_NOT_FOUND

X509 RSASSA-PSS parameters ASN1 (MGAlg.params.params NULL)
depends_on:MBEDTLS_RSA_C:MBEDTLS_SHA256_C
x509_parse_rsassa_pss_params:"A11C301A06092A864886F70D010108300D06096086480165030402010500":MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA256:20:0

X509 RSASSA-PSS parameters ASN1 (MGAlg.params.params wrong tag)
depends_on:MBEDTLS_RSA_C:MBEDTLS_SHA256_C
x509_parse_rsassa_pss_params:"A11C301A06092A864886F70D010108300D06096086480165030402013000":MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA256:20:MBEDTLS_ERR_X509_INVALID_ALG + MBEDTLS_ERR_ASN1_UNEXPECTED_TAG

X509 RSASSA-PSS parameters ASN1 (MGAlg.params wrong len #1c)
x509_parse_rsassa_pss_params:"A11D301B06092A864886F70D010108300E06096086480165030402010500":MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA256:20:MBEDTLS_ERR_X509_INVALID_ALG

+ MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 RSASSA-PSS parameters ASN1 (MGAlg.params wrong len #2)
depends_on:MBEDTLS_RSA_C:MBEDTLS_SHA256_C
x509_parse_rsassa_pss_params:"A11D301B06092A864886F70D010108300E06096086480165030402010500
00":MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA256:20:MBEDTLS_ERR_X509_I
NVALID_ALG + MBEDTLS_ERR_ASN1_LENGTH_MISMATCH

X509 RSASSA-PSS parameters ASN1 (good, saltLen = 94)
x509_parse_rsassa_pss_params:"A20302015E":MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:94:0

X509 RSASSA-PSS parameters ASN1 (good, explicit saltLen = default)
x509_parse_rsassa_pss_params:"A203020114":MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:20:0

X509 RSASSA-PSS parameters ASN1 (saltLen wrong len #1)
x509_parse_rsassa_pss_params:"A20402015E":MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:94:MBEDTLS_ERR_X509_IN
VALID_ALG
+ MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 RSASSA-PSS parameters ASN1 (saltLen wrong len #2)
x509_parse_rsassa_pss_params:"A20402015E00":MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:94:MBEDTLS_ERR_X509_IN
VALID_ALG + MBEDTLS_ERR_ASN1_LENGTH_MISMATCH

X509 RSASSA-PSS parameters ASN1 (saltLen not an int)
x509_parse_rsassa_pss_params:"A2023000":MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:94:MBEDTLS_ERR_X509_IN
VALID_ALG + MBEDTLS_ERR_ASN1_UNEXPECTED_TAG

X509 RSASSA-PSS parameters ASN1 (good, explicit trailerField = default)
x509_parse_rsassa_pss_params:"A303020101":MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:20:0

X509 RSASSA-PSS parameters ASN1 (trailerField wrong len #1)
x509_parse_rsassa_pss_params:"A304020101":MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:20:MBEDTLS_ERR_X509_IN
VALID_ALG + MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509
RSASSA-PSS parameters ASN1 (trailerField wrong len #2)
x509_parse_rsassa_pss_params:"A30402010100":MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:20:MBEDTLS_ERR_X509_IN
VALID_ALG + MBEDTLS_ERR_ASN1_LENGTH_MISMATCH

X509 RSASSA-PSS parameters ASN1 (trailerField not an int)
x509_parse_rsassa_pss_params:"A3023000":MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:20:MBEDTLS_ERR_X509_IN
VALID_ALG + MBEDTLS_ERR_ASN1_UNEXPECTED_TAG

X509 RSASSA-PSS parameters ASN1 (trailerField not 1)
x509_parse_rsassa_pss_params:"A303020102":MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:20:MBEDTLS_ERR_X509_IN
VALID_ALG

X509 CSR ASN.1 (OK)
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA1_C
mbedtls_x509_csr_parse:"308201183081BF0201003034310B300906035504061302E4C3111300F060355040A13
08506F6C617253534C311230100603554031306C6F63616C686F737430593013060072A8648CE3D020106082A
8648CE3D030107034200437CC56D976091E5A723EC7592DFF206EEE7CF9069174D0AD14B5F76822596292
4EE500D82311FFEA2FD2345D5D16BD8A88C26B770D55CD8A2A0EFA01C8B4EDFFA029302706092A86488
6F70D01090E311A301830090603551D1304023000300B0603551D0F0404030205E0300906072A8648CE3D0401
0349003046022100B49FD8C8F77ABFA871908DFBE684A08A793D0F490A43D86FCF2086E4F24BB0C202210
0F829D5CCD3742369299E6294394717C4B723A0F68B44E831B6E6C3BCABF97243":"CSR
 version   \: 1\nsubject name \: C=NL, O=PolarSSL, CN=localhost\nsigned using \: ECDSA with SHA1\nEC key
size   \: 256 bits\n":0

X509 CSR ASN.1 (bad first tag)
mbedtls_x509_csr_parse:"3100":"":MBEDTLS_ERR_X509_INVALID_FORMAT

X509 CSR ASN.1 (bad sequence: overlong)
mbedtls_x509_csr_parse:"3001":"":MBEDTLS_ERR_X509_INVALID_FORMAT

X509 CSR ASN.1 (total length mistmatch)
mbedtls_x509_csr_parse:"30010000":"":MBEDTLS_ERR_X509_INVALID_FORMAT +
MBEDTLS_ERR_ASN1_LENGTH_MISMATCH

X509 CSR ASN.1 (bad CRI: not a sequence)
mbedtls_x509_csr_parse:"30023100":"":MBEDTLS_ERR_X509_INVALID_FORMAT +
MBEDTLS_ERR_ASN1_UNEXPECTED_TAG

X509
 CSR ASN.1 (bad CRI: overlong)
mbedtls_x509_csr_parse:"30023001":"":MBEDTLS_ERR_X509_INVALID_FORMAT +
MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 CSR ASN.1 (bad CRI.Version: overlong)
mbedtls_x509_csr_parse:"30053002020100":"":MBEDTLS_ERR_X509_INVALID_VERSION +
MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 CSR ASN.1 (bad CRI.Version: not v1)
mbedtls_x509_csr_parse:"30053003020101":"":MBEDTLS_ERR_X509_UNKNOWN_VERSION

X509 CSR ASN.1 (bad CRI.Name: not a sequence)
mbedtls_x509_csr_parse:"300730050201003100":"":MBEDTLS_ERR_X509_INVALID_FORMAT +
MBEDTLS_ERR_ASN1_UNEXPECTED_TAG

X509 CSR ASN.1 (bad CRI.Name: overlong)
mbedtls_x509_csr_parse:"30083005020100300100":"":MBEDTLS_ERR_X509_INVALID_FORMAT +
MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 CSR ASN.1 (bad CRI.Name payload: not a set)
mbedtls_x509_csr_parse:"3009300702010030023000":"":MBEDTLS_ERR_X509_INVALID_NAME +
MBEDTLS_ERR_ASN1_UNEXPECTED_TAG

X509 CSR ASN.1 (bad CRI.Name payload: overlong)
mbedtls_x509_csr_parse:"300A30080201003002310100":"":MBEDTLS_ERR_X509_INVALID_NAME
+ MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 CSR ASN.1 (bad SubjectPublicKeyInfo: missing)
mbedtls_x509_csr_parse:"30143012020100300D310B300906035504061302 4E4C":"":MBEDTLS_ERR_PK_KEY
_INVALID_FORMAT + MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 CSR ASN.1 (bad SubjectPublicKeyInfo: not a sequence)
mbedtls_x509_csr_parse:"30163014020100300D310B300906035504061302 4E4C3100":"":MBEDTLS_ERR_PK_
KEY_INVALID_FORMAT + MBEDTLS_ERR_ASN1_UNEXPECTED_TAG

X509 CSR ASN.1 (bad SubjectPublicKeyInfo: overlong)
mbedtls_x509_csr_parse:"30173014020100300D310B300906035504061302 4E4C300100":"":MBEDTLS_ERR_P
K_KEY_INVALID_FORMAT + MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 CSR ASN.1 (bad attributes: missing)
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED
mbedtls_x509_csr_parse:"308197308194020100303431 0B300906035504061302 4E4C3111300F060355040A1308
506F6C617253534C311230100603550403130 96C6F63616C686F73743059301306072A8648CE3D020106082A86
48CE3D030107034200043 7CC56D976091E5A723EC7592DFF206EEE7CF9069174D0AD14B5F768225962924E
E500D82311FFEA2FD2345D5D16BD8A88C26B770D55CD8A2A0EFA01C8B4EDFF":"":MBEDTLS_ERR_X50
9_INVALID_FORMAT
+ MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 CSR ASN.1 (bad attributes: bad tag)
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED
mbedtls_x509_csr_parse:"308199308196020100303431 0B300906035504061302 4E4C3111300F060355040A1308
506F6C617253534C311230100603550403130 96C6F63616C686F73743059301306072A8648CE3D020106082A86
48CE3D030107034200043 7CC56D976091E5A723EC7592DFF206EEE7CF9069174D0AD14B5F768225962924E
E500D82311FFEA2FD2345D5D16BD8A88C26B770D55CD8A2A0EFA01C8B4EDFF0500":"":MBEDTLS_ERR
_X509_INVALID_FORMAT + MBEDTLS_ERR_ASN1_UNEXPECTED_TAG

X509 CSR ASN.1 (bad attributes: overlong)
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED
mbedtls_x509_csr_parse:"30819A308196020100303431 0B300906035504061302 4E4C3111300F060355040A1308

506F6C617253534C31123010060355040313096C6F63616C686F73743059301306072A8648CE3D020106082A86
48CE3D030107034200043CC56D976091E5A723EC7592DFF206EEE7CF9069174D0AD14B5F768225962924E
E500D82311FFEA2FD2345D5D16BD8A88C26B770D55CD8A2A0EFA01C8B4EDFFA00100":"":MBEDTLS_E
RR_X509_INVALID_FORMAT
+ MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 CSR ASN.1 (bad sigAlg: missing)
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED
mbedtls_x509_csr_parse:"3081C23081BF0201003034310B300906035504061302E4C3111300F060355040A1308
506F6C617253534C31123010060355040313096C6F63616C686F73743059301306072A8648CE3D020106082A86
48CE3D030107034200043CC56D976091E5A723EC7592DFF206EEE7CF9069174D0AD14B5F768225962924E
E500D82311FFEA2FD2345D5D16BD8A88C26B770D55CD8A2A0EFA01C8B4EDFFA029302706092A864886F
70D01090E311A301830090603551D1304023000300B0603551D0F0404030205E0":"":MBEDTLS_ERR_X509_I
NVALID_ALG + MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 CSR ASN.1 (bad sigAlg: not a sequence)
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED
mbedtls_x509_csr_parse:"3081C43081BF0201003034310B300906035504061302E4C3111300F060355040A1308
506F6C617253534C31123010060355040313096C6F63616C686F73743059301306072A8648CE3D020106082A86
48CE3D030107034200043CC56D976091E5A723EC7592DFF206EEE7CF9069174D0AD14B5F768225962924E
E500D82311FFEA2FD2345D5D16BD8A88C26B770D55CD8A2A0EFA01C8B4EDFFA029302706092A864886F
70D01090E311A301830090603551D1304023000300B0603551D0F0404030205E03100":"":MBEDTLS_ERR_X5
09_INVALID_ALG
+ MBEDTLS_ERR_ASN1_UNEXPECTED_TAG

X509 CSR ASN.1 (bad sigAlg: overlong)
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED
mbedtls_x509_csr_parse:"3081C43081BF0201003034310B300906035504061302E4C3111300F060355040A1308
506F6C617253534C31123010060355040313096C6F63616C686F73743059301306072A8648CE3D020106082A86
48CE3D030107034200043CC56D976091E5A723EC7592DFF206EEE7CF9069174D0AD14B5F768225962924E
E500D82311FFEA2FD2345D5D16BD8A88C26B770D55CD8A2A0EFA01C8B4EDFFA029302706092A864886F
70D01090E311A301830090603551D1304023000300B0603551D0F0404030205E03001":"":MBEDTLS_ERR_X5
09_INVALID_ALG + MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 CSR ASN.1 (bad sigAlg: unknown)
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED
mbedtls_x509_csr_parse:"3081CD3081BF0201003034310B300906035504061302E4C3111300F060355040A130
8506F6C617253534C31123010060355040313096C6F63616C686F73743059301306072A8648CE3D020106082A8
648CE3D030107034200043CC56D976091E5A723EC7592DFF206EEE7CF9069174D0AD14B5F768225962924
EE500D82311FFEA2FD2345D5D16BD8A88C26B770D55CD8A2A0EFA01C8B4EDFFA029302706092A864886
F70D01090E311A301830090603551D1304023000300B0603551D0F0404030205E0300906072A8648CE3D04FF"
:"":MBEDTLS_ERR_X509_UNKNOWN_SIG_ALG

X509
CSR ASN.1 (bad sig: missing)
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA1_C
mbedtls_x509_csr_parse:"3081CD3081BF0201003034310B300906035504061302E4C3111300F060355040A130
8506F6C617253534C31123010060355040313096C6F63616C686F73743059301306072A8648CE3D020106082A8

648CE3D0301070342000437CC56D976091E5A723EC7592DFF206EEE7CF9069174D0AD14B5F768225962924
EE500D82311FFEA2FD2345D5D16BD8A88C26B770D55CD8A2A0EFA01C8B4EDFFA029302706092A864886
F70D01090E311A301830090603551D1304023000300B0603551D0F0404030205E0300906072A8648CE3D0401":
"":MBEDTLS_ERR_X509_INVALID_SIGNATURE
+ MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 CSR ASN.1 (bad sig: not a bit string)
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA1_C
mbedtls_x509_csr_parse:"3081CF3081BF0201003034310B300906035504061302E4C3111300F060355040A1308
506F6C617253534C311230100603550403096C6F63616C686F73743059301306072A8648CE3D020106082A86
48CE3D0301070342000437CC56D976091E5A723EC7592DFF206EEE7CF9069174D0AD14B5F768225962924E
E500D82311FFEA2FD2345D5D16BD8A88C26B770D55CD8A2A0EFA01C8B4EDFFA029302706092A864886F
70D01090E311A301830090603551D1304023000300B0603551D0F0404030205E0300906072A8648CE3D040104
00":"":MBEDTLS_ERR_X509_INVALID_SIGNATURE + MBEDTLS_ERR_ASN1_UNEXPECTED_TAG

X509 CSR ASN.1 (bad sig: overlong)
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA1_C
mbedtls_x509_csr_parse:"3081CF3081BF0201003034310B300906035504061302E4C3111300F060355040A1308
506F6C617253534C311230100603550403096C6F63616C686F73743059301306072A8648CE3D020106082A86
48CE3D0301070342000437CC56D976091E5A723EC7592DFF206EEE7CF9069174D0AD14B5F768225962924E
E500D82311FFEA2FD2345D5D16BD8A88C26B770D55CD8A2A0EFA01C8B4EDFFA029302706092A864886F
70D01090E311A301830090603551D1304023000300B0603551D0F0404030205E0300906072A8648CE3D040103
01":"":MBEDTLS_ERR_X509_INVALID_SIGNATURE
+ MBEDTLS_ERR_ASN1_OUT_OF_DATA

X509 CSR ASN.1 (extra data after signature)
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA1_C
mbedtls_x509_csr_parse:"308201193081BF0201003034310B300906035504061302E4C3111300F060355040A13
08506F6C617253534C311230100603550403096C6F63616C686F73743059301306072A8648CE3D020106082A
8648CE3D0301070342000437CC56D976091E5A723EC7592DFF206EEE7CF9069174D0AD14B5F76822596292
4EE500D82311FFEA2FD2345D5D16BD8A88C26B770D55CD8A2A0EFA01C8B4EDFFA029302706092A86488
6F70D01090E311A301830090603551D1304023000300B0603551D0F0404030205E0300906072A8648CE3D0401
0349003046022100B49FD8C8F77ABFA871908DFBE684A08A793D0F490A43D86FCF2086E4F24BB0C202210
0F829D5CCD3742369299E6294394717C4B723A0F68B44E831B6E6C3BCABF9724300":"":MBEDTLS_ERR_X
509_INVALID_FORMAT
+ MBEDTLS_ERR_ASN1_LENGTH_MISMATCH

X509 CSR ASN.1 (invalid version overflow)
mbedtls_x509_csr_parse:"3008300602047FFFFFFF":"":MBEDTLS_ERR_X509_UNKNOWN_VERSION

X509 File parse (no issues)
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA256_C
x509parse_crt_file:"data_files/server7_int-ca.crt":0

X509 File parse (extra space in one certificate)
depends_on:MBEDTLS_ECP_C:MBEDTLS_SHA256_C
x509parse_crt_file:"data_files/server7_pem_space.crt":1

X509 File parse (all certificates fail)
depends_on:MBEDTLS_ECP_C
x509parse_crt_file:"data_files/server7_all_space.crt":MBEDTLS_ERR_PEM_INVALID_DATA +
MBEDTLS_ERR_BASE64_INVALID_CHARACTER

X509 File parse (trailing spaces, OK)
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA256_C
x509parse_crt_file:"data_files/server7_trailing_space.crt":0

X509 Get time (UTC no issues)
depends_on:MBEDTLS_X509_USE_C
x509_get_time:MBEDTLS_ASN1_UTC_TIME:"500101000000Z":0:1950:1:1:0:0:0

X509
Get time (Generalized Time no issues)
depends_on:MBEDTLS_X509_USE_C
x509_get_time:MBEDTLS_ASN1_GENERALIZED_TIME:"99991231235959Z":0:9999:12:31:23:59:59

X509 Get time (UTC year without leap day)
depends_on:MBEDTLS_X509_USE_C
x509_get_time:MBEDTLS_ASN1_UTC_TIME:"490229121212Z":MBEDTLS_ERR_X509_INVALID_DATE:0:0
:0:0:0:0

X509 Get time (UTC year with leap day)
depends_on:MBEDTLS_X509_USE_C
x509_get_time:MBEDTLS_ASN1_UTC_TIME:"000229121212Z":0:2000:2:29:12:12:12

X509 Get time (UTC invalid day of month #1)
depends_on:MBEDTLS_X509_USE_C
x509_get_time:MBEDTLS_ASN1_UTC_TIME:"000132121212Z":MBEDTLS_ERR_X509_INVALID_DATE:0:0
:0:0:0:0

X509 Get time (UTC invalid day of month #2)
depends_on:MBEDTLS_X509_USE_C
x509_get_time:MBEDTLS_ASN1_UTC_TIME:"001131121212Z":MBEDTLS_ERR_X509_INVALID_DATE:0:0
:0:0:0:0

X509 Get time (UTC invalid hour)
depends_on:MBEDTLS_X509_USE_C
x509_get_time:MBEDTLS_ASN1_UTC_TIME:"001130241212Z":MBEDTLS_ERR_X509_INVALID_DATE:0:0
:0:0:0:0

X509
Get time (UTC invalid min)
depends_on:MBEDTLS_X509_USE_C
x509_get_time:MBEDTLS_ASN1_UTC_TIME:"001130236012Z":MBEDTLS_ERR_X509_INVALID_DATE:0:0
:0:0:0:0

X509 Get time (UTC invalid sec)
depends_on:MBEDTLS_X509_USE_C
x509_get_time:MBEDTLS_ASN1_UTC_TIME:"001130235960Z":MBEDTLS_ERR_X509_INVALID_DATE:0:0:0:0:0:0

X509 Get time (UTC without time zone)
depends_on:MBEDTLS_X509_USE_C
x509_get_time:MBEDTLS_ASN1_UTC_TIME:"000229121212":0:2000:2:29:12:12:12

X509 Get time (UTC with invalid time zone #1)
depends_on:MBEDTLS_X509_USE_C
x509_get_time:MBEDTLS_ASN1_UTC_TIME:"000229121212J":MBEDTLS_ERR_X509_INVALID_DATE:0:0:0:0:0:0

X509 Get time (UTC with invalid time zone #2)
depends_on:MBEDTLS_X509_USE_C
x509_get_time:MBEDTLS_ASN1_UTC_TIME:"000229121212+0300":MBEDTLS_ERR_X509_INVALID_DATE:0:0:0:0:0:0

X509 Get time (Date with invalid tag)
depends_on:MBEDTLS_X509_USE_C
x509_get_time:MBEDTLS_ASN1_CONTEXT_SPECIFIC:"000229121212":MBEDTLS_ERR_X509_INVALID_DATE+MBEDTLS_ERR_ASN1_UNEXPECTED_TAG:0:0:0:0:0:0

X509
Get time (UTC, truncated)
depends_on:MBEDTLS_X509_USE_C
x509_get_time:MBEDTLS_ASN1_UTC_TIME:"000229121":MBEDTLS_ERR_X509_INVALID_DATE:0:0:0:0:0:0

X509 Get time (Generalized Time, truncated)
depends_on:MBEDTLS_X509_USE_C
x509_get_time:MBEDTLS_ASN1_GENERALIZED_TIME:"20000229121":MBEDTLS_ERR_X509_INVALID_DATE:0:0:0:0:0:0

X509 Get time (UTC without seconds)
depends_on:MBEDTLS_X509_USE_C
x509_get_time:MBEDTLS_ASN1_UTC_TIME:"0002291212":MBEDTLS_ERR_X509_INVALID_DATE:2000:2:29:12:12:0

X509 Get time (UTC without seconds and with invalid time zone #1)
depends_on:MBEDTLS_X509_USE_C
x509_get_time:MBEDTLS_ASN1_UTC_TIME:"0002291212J":MBEDTLS_ERR_X509_INVALID_DATE:0:0:0:0:0:0

X509 Get time (UTC without second and with invalid time zone #2)
depends_on:MBEDTLS_X509_USE_C
x509_get_time:MBEDTLS_ASN1_UTC_TIME:"0002291212+0300":MBEDTLS_ERR_X509_INVALID_DATE:0

:0:0:0:0:0

X509 Get time (UTC invalid character in year)
depends_on:MBEDTLS_X509_USE_C
x509_get_time:MBEDTLS_ASN1_UTC_TIME:"0\1130231212Z":MBEDTLS_ERR_X509_INVALID_DATE:0:0:0:0:0:0

X509
Get time (UTC invalid character in month)
depends_on:MBEDTLS_X509_USE_C
x509_get_time:MBEDTLS_ASN1_UTC_TIME:"001%30231212Z":MBEDTLS_ERR_X509_INVALID_DATE:0:0:0:0:0:0

X509 Get time (UTC invalid character in day)
depends_on:MBEDTLS_X509_USE_C
x509_get_time:MBEDTLS_ASN1_UTC_TIME:"0011`0231212Z":MBEDTLS_ERR_X509_INVALID_DATE:0:0:0:0:0:0

X509 Get time (UTC invalid character in hour)
depends_on:MBEDTLS_X509_USE_C
x509_get_time:MBEDTLS_ASN1_UTC_TIME:"0011302h1212Z":MBEDTLS_ERR_X509_INVALID_DATE:0:0:0:0:0:0

X509 Get time (UTC invalid character in min)
depends_on:MBEDTLS_X509_USE_C
x509_get_time:MBEDTLS_ASN1_UTC_TIME:"00113023u012Z":MBEDTLS_ERR_X509_INVALID_DATE:0:0:0:0:0:0

X509 Get time (UTC invalid character in sec)
depends_on:MBEDTLS_X509_USE_C
x509_get_time:MBEDTLS_ASN1_UTC_TIME:"0011302359n0Z":MBEDTLS_ERR_X509_INVALID_DATE:0:0:0:0:0:0
This directory contains the certificates for the tests targeting the enforcement of the policy indicated by the *pathLenConstraint* field. All leaf elements were generated with *is_ca* unset and all roots with the *selfsign=1* option.

1. zero pathlen constraint on an intermediate CA (invalid)
```
cert11.crt -> cert12.crt (max_pathlen=0) -> cert13.crt -> cert14.crt
```

2. zero pathlen constraint on the root CA (invalid)
```
cert21.crt (max_pathlen=0) -> cert22.crt -> cert23.crt
```

3. nonzero pathlen constraint on the root CA (invalid)
```
```

cert31.crt (max_pathlen=1) -> cert32.crt -> cert33.crt -> cert34.crt
```

4. nonzero pathlen constraint on an intermediate CA (invalid)
```
cert41.crt -> cert42.crt (max_pathlen=1) -> cert43.crt -> cert44.crt -> cert45.crt
```

5. nonzero pathlen constraint on an intermediate CA with maximum number of elements in the chain (valid)
```
cert51.crt -> cert52.crt (max_pathlen=1) -> cert53.crt -> cert54.crt
```

6. nonzero pathlen constraint on the root
CA with maximum number of elements in the chain (valid)
```
cert61.crt (max_pathlen=1) -> cert62.crt -> cert63.crt
```

7. pathlen constraint on the root CA with maximum number of elements and a self signed certificate in the chain (valid)
(This situation happens for example when a root of some hierarchy gets integrated into another hierarchy. In this case the certificates issued before the integration will have an intermadiate self signed certificate in their chain)
```
cert71.crt (max_pathlen=1) -> cert72.crt -> cert73.crt (self signed) -> cert74.crt -> cert74.crt
```

8. zero pathlen constraint on first intermediate CA (valid)
```
cert81.crt -> cert82.crt (max_pathlen=0) -> cert83.crt
```

9. zero pathlen constraint on trusted root (valid)
```
cert91.crt (max_pathlen=0) -> cert92.crt
```
-----BEGIN CERTIFICATE-----
MIIBoDCCAUWgAwIBAgIBUzAMBggqhkjOPQQDAgUAMDExDzANBgNVBAMTBkludCA4
MjERMA8GA1UEChMIbWJlZCBUTFMxCzAJBgNVBAYTAlVLMB4XDTAxMDEwMTAwMDAw
MFoXDTMwMTIzMTIzNTk1OVowMDEOMAwGA1UEAxMFRUUgODMxETAPBgNVBAoTCG1i
ZWQgVExTMQswCQYDVQQGEwJVSzBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABMSy
6X5iBYrdxxOMfdcA23pLBoJCeyEjiWfALxTm80MJGBdRNVdnT50xNU3SDDwHWPda
/EQqHq+itsqkUeyAGAyjTTBLMAkGA1UdEwQCMAAwHQYDVR0OBBYEFGsFH/KsvM4n
r+i1gI2iCVXi3KtFMB8GA1UdIwQYMBaAFLf6ey/edCSdKDhoOOVOJGkI+jtfMAwG
CCqGSM49BAMCBQADRwAwRAIgQURH8DHWFHVK38+znWc85G1P+g4ocdkA5Gt0LbOg
SJMCIBsacOLFywxZYF8atizw6zMRw+QeHR2514JIhJUck2kd
-----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----
MIIDCjCCAfKgAwIBAgIBATANBgkqhkiG9w0BAQsFADAWMRQwEgYDVQQDEwtUZXN0
IHJvb3QgNDAeFw0wMTAxMDEwMDAwMDBaFw0zMDEyMzEyMzU5NTlaMCYxJDAiBgNV
BAMTG1Rlc3QgaW50ZXJtZWRpYXRlIG1heHBhdGggMTCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBANpGlBMXdo8cO9oqUw/b6PMwiMNV8LCe6wB9VKHPa6OG
Q0o8Xqktgwnh1rojgpMhbCApE7UXeMr6ZGq/NtqmO1hO5adV5JehWZyvg7j4EBpG
g8iWo0jNpKMJ0Yx1uBkkljEdZLTHa4bK/zy2NKqDNS2yWs9/M5+xw5XE2ecAg7FT
cXhf3q50V+M6T2IaQ9BxntTyCT8IIF2eRM/t9Y944s9Rfzm/KQVKRYPudX7YhTt9
iqCJB4JoqYhs3HEO0wPkJxY4KBTUCN94s+7jUFdRrYxe+8Ya6tIYWqD38i5qdGhY
xrVey1LatsDJQ2EgNYobM/LjoCLK1WUssEqf0OU2bi0CAwEAAaNTMFEwDwYDVR0T
BAgwBgEBAQIBATAdBgNVHQ4EFgQUOBl8edVm/H5xdS2EGEeLzftZ/DUwHwYDVR0j
BBgwFoAUjgXdXx9NGPa+UvHBC4//SE+ARpQwDQYJKoZIhvcNAQELBQADggEBAGKh
pBhYSGN0KGWIG4GG4mVoTiw880ehetDuTpl3ymZNqkoUuTaAtU3PJWOctcJva7h6
4PSgyabi/WQmhntR1GxCUt0GTuhHmyJYsSwakXUgMgF6W6TKcxg6m4vjMkkrf+ZT
1lO/MiwxhTTluHPGkl/nBG+uxySInuQMDvdyQDXp2e17qxops+G+1UnRJinqLtsd
LMkCOT4pyh6B5ysnJ8gP1Z2EKWjhKJcIHRMUm7Ap/pf8Zgh5LIqdRtDSuNuTmPLP
lkgoebOCO3c/mWCciR0xGCcz86G3fYznvGp4XqHnRkg3SpAcHQbQ/nSHA+1LdfFi
nqZQPnJPVsJctDR935c=
-----END
 CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIICIDCCAaWgAwIBAgIBEzAKBggqhkjOPQQDATA+MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EwHhcN
MTMwOTI0MTYyMTI3WhcNMjMwOTIyMTYyMTI3WjA0MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxEjAQBgNVBAMTCWxvY2FsaG9zdDBZMBMGByqGSM49AgEG
CCqGSM49AwEHA0IABDfMVtl2CR5acj7HWS3/IG7ufPkGkXTQrRS192giWWKSTuUA
2CMR/+ov0jRdXRa9iojCa3cNVc2KKg76Aci07f+jgZ0wgZowCQYDVR0TBAIwADAd
BgNVHQ4EFgQUUGGlj9QH2deCAQzlZX+MY0anE74wbgYDVR0jBGcwZYAUnW0gJEkB
PyvLeLUZvH4kydv7NnyhQqRAMD4xCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQb2xh
clNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBFQyBDQYIJAMFD4n5iQ8zoMAoG
CCqGSM49BAMBA2kAMGYCMQCj0EyFUzDRmfokWzLVEWN0epR4/sZytfIeozp6BqWH
qaTBdAR2vthIKC7dKuUkg34CMQD6YtB2O9Vso79gbzSen2qh7gK7VvGE+31EVPbR
Ce/oNG/3OfhRSdn3FOvBBg2UErM=
-----END CERTIFICATE-----
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
```

```
    <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
    <Configuration>Release</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
</ItemGroup>
<ItemGroup>
  <ClCompile Include="..\..\programs\util\pem2der.c" />
</ItemGroup>
<ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">

 <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
</ItemGroup>
<PropertyGroup Label="Globals">
  <ProjectGuid>{D3C6FBD6-D78E-7180-8345-5E09B492DBEC}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>pem2der</RootNamespace>
</PropertyGroup>
<Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
</PropertyGroup>
<Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
<ImportGroup Label="ExtensionSettings">
</ImportGroup>
```

```
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
 />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
    <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
   <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <LinkIncremental>false</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
   <LinkIncremental>false</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <ClCompile>
     <PrecompiledHeader>
     </PrecompiledHeader>
     <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
      <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
     <SubSystem>Console</SubSystem>
     <GenerateDebugInformation>true</GenerateDebugInformation>
     <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
```

2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
<AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
</Link>
<ProjectReference>
<LinkLibraryDependencies>false</LinkLibraryDependencies>
</ProjectReference>
</ItemDefinitionGroup>
<ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
<ClCompile>
<PrecompiledHeader>
</PrecompiledHeader>
<WarningLevel>Level3</WarningLevel>
<Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
<AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
</ClCompile>
<Link>
<SubSystem>Console</SubSystem>
<GenerateDebugInformation>true</GenerateDebugInformation>
<ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
<AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
</Link>
<ProjectReference>
<LinkLibraryDependencies>false</LinkLibraryDependencies>
</ProjectReference>
</ItemDefinitionGroup>
<ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
<ClCompile>
<WarningLevel>Level3</WarningLevel>
<PrecompiledHeader>
</PrecompiledHeader>
<Optimization>MaxSpeed</Optimization>
<FunctionLevelLinking>true</FunctionLevelLinking>
<IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
<AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
</ClCompile>
<Link>
<SubSystem>Console</SubSystem>
<GenerateDebugInformation>true</GenerateDebugInformation>
<EnableCOMDATFolding>true</EnableCOMDATFolding>
<OptimizeReferences>true</OptimizeReferences>
<AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3

2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.targets"
 />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
-----BEGIN CERTIFICATE-----
MIIDDDCCAfSgAwIBAgIBATANBgkqhkiG9w0BAQsFADAmMSQwIgYDVQQDExtUZXN0
IGludGVybWVkaWF0ZSBtYXhwYXRoIDIwHhcNMDEwMTAxMDAwMDAwWhcNMzAxMjMx
MjM1OTU5WjAeMRwwGgYDVQQDExNUZXN0IGxlYWYgaW52YWxpZCAzMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAkSrgWFD4lYQ0RF/z3mJZjn1lgNBkhnCP
0hciJv/etoMN3bCB+uc8fo0wxDQ2ZcbzTAQ0qBNnjJvAJ1qslZA9boIBKmT8JSix
ii/1XTDWI3E5aOvX1h6lW66pVsIzLm0NAf0VJn2xLw0Yv8hfKbwjcNeAfm7GCwJB
8skjekMKJ8+e6pP4ZHxmrnOo0kUlCg8w8RKzZ6sYJxX1ETekWPEUSXrscQ/YSjpO
zjLDph1lO4gVErBhdJgJpJznqkrRBiR7f/hIrpAV3wOUbtfrxrIb5FXOM9rt/svW
RRrzIUGnBvo04WZ+KQHPsMn+9x8i+/tueOg1KLfs10hW0RWsTQjmOQIDAQABo00w
SzAJBgNVHRMEAjAAMB0GA1UdDgQWBBSOBr1U4h5PYyOqGe/gJgwWk7FfezAfBgNV
HSMEGDAWgBTCN2vDLY1tcenTzyRmlS4TBe2xijANBgkqhkiG9w0BAQsFAAOCAQEA
aBLuwNN5vOh2dLbn8lMNsc/oTFSInzu+ylzC/KLTkjoyMYY+S2ISUuew9pzUo4Gs
AAE/rqVYednayyA13eNRBnwIw+8kPTESaJMGl6uQQd8DzAalzqxbFhbwFY2T0pdi
LNFkGjmGdpRNy/VSTy6JEEBMhIKXjMpactmpiV6mwK3bfnFaXZ6o70+JZrNeiSe0
g8sci6gBVEt27bGvhLalut8WXc7VCkxQhQCSBdv/94EmRxzPye6iAK0L9jaTHlt+
qR5MWJxZN32muI7nsKnetUMZbIYwvO1LPn8f+0hdYkck8kE7ga1UM98oTgQeIOmj
3JNCDkNY+Z387ujaaOAVxw==
-----END

CERTIFICATE-----
-----BEGIN X509 CRL-----
MIIBqzCBlDANBgkqhkiG9w0BAQ0FADA7MQswCQYDVQQGEwJOTDERMA8GA1UEChMI
UG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EXDTExMDIxMjE0NDQw
N1oXDTExMDQxMzE0NDQwN1owKDASAgEBFw0xMTAyMTIxNDQ0MDdaMBICAQMXDTEx
MDIxMjE0NDQwN1owDQYJKoZIhvcNAQENBQADggEBAH6GU24hd6d/5PmDusT+h2Kl
e7scmhkZDPU+VJSnzHdEREYTPaoFqyVBuJOE95lZELEqdOauhO3lG2WEQVGcgEcv
4jS2EzR3BYex1c1upqGtdIvIoA9TOLukdy6KeauomiWho2Kd7bSaXHy20jwdkLko
/t3lVhTtBvKbh8XHVYwCaw1aCj3LydwNcS+zPnRgsMVHszFxmMNn5HCRW8lbYwcf
UA98OmxIZs2hpBKRpvlfA5y6sXEx2+tSMg+MJrziGBgG6OR/m+KTaK5Yle9nrC+7
hzKIe83hpktvfB1CY5Ak4Uke9/1FRqAjs5KCRxYSGQ7ZdS7DgAeGwT3slLbl/tY=
-----END X509 CRL-----
AES-ECB Encrypt (Invalid keylength)
aes_encrypt_ecb:"00000000000000000000000000000000":"f34481ec3cc627bacd5dc3fb08f273e6":"0336763e966d92595a567cc9ce537f5e":MBEDTLS_ERR_AES_INVALID_KEY_LENGTH

AES-ECB Decrypt (Invalid keylength)
aes_decrypt_ecb:"00000000000000000000000000000000":"f34481ec3cc627bacd5dc3fb08f273e6":"0336763e966d92595a567cc9ce537f5e":MBEDTLS_ERR_AES_INVALID_KEY_LENGTH

AES-256-CBC Encrypt (Invalid input length)
aes_encrypt_cbc:"0000000000000000000000000000000000000000000000000000000000000000":"00000000000000000000000000000000":"fffffffffffffe000000000000000":"":MBEDTLS_ERR_AES_INVALID_INPUT_LENGTH

AES-256-CBC Decrypt (Invalid input length)
aes_decrypt_cbc:"0000000000000000000000000000000000000000000000000000000000000000":"00000000000000000000000000000000":"623a52fcea5d443e48d9181ab32c74":"":MBEDTLS_ERR_AES_INVALID_INPUT_LENGTH

AES Selftest
depends_on:MBEDTLS_SELF_TEST
aes_selftest:
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
   <Platform>Win32</Platform>

```
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
    <Configuration>Release</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
</ItemGroup>
<ItemGroup>
  <ClCompile Include="..\..\programs\test\udp_proxy.c" />
</ItemGroup>
<ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">

    <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
</ItemGroup>
<PropertyGroup Label="Globals">
  <ProjectGuid>{7E2C80FE-3CC3-82B4-0CAD-65DC233DE13A}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>udp_proxy</RootNamespace>
</PropertyGroup>
<Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
    <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
</PropertyGroup>
<Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
<ImportGroup Label="ExtensionSettings">
</ImportGroup>
<ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
```

```
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
 />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
     <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
```

```
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
```

```
cies>
  </Link>
 </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
 <Import
 Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDcwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDgwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAARpQeQ/YGQj
nl7Szo6WStJ1u7xunTL5jBkXH8aAVSm0qiX4AD/7YPxa5EnGzZdLTn25vQVnfQAG
pMx8P1lYiGYCo4GJMIGGMB0GA1UdDgQWBBS40mLt93U8Sh8ZGiDVAhRSiBPcXjBX
BgNVHSMEUDBOgBREq5J3toJPxZ3O+ssJ5vkkU0RJE6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA2ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhANwGf+F4a+kmXWz8UjSpRkaToTV6EFWw
/Tjzj0tQhDoAAiEA19RxeWOVBBpM6LOHg6v5Lf54YN1snkLf+sEXyZCuWQQ=
-----END CERTIFICATE-----
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIE6jAcBgoqhkiG9w0BDAEDMA4ECGhNuQogiktrAgIIAASCBMhfcb+Jt0YOgGni
IWnwmmtYT6Nvina/j3FCGzcHCDyUQDqh1rPUtZnmUdM3fyEGlUJdX9wmHh3gUkWx
JE00QMzYDQsUbGrt8H3rCQ+aXegCicXAyBgDh0YUhO7bWmgJNSvZOduIeCJ81mnb
xtl3CGgaYVOWspr458crtvn1Hlhq0EGs54EUHWBE89PHNxokGHqkFQcdp7QHO9Zm
ZvjTn+kR0K5KQbeQwMf3LcboueDV71ueUZsHlTSZ5Qs7WZORRzMBoo2SWV+Mh7U/
yAQv4i6CMauVifVqTMbLtfdTyZCts3N57sGstyqIruE1Jwg8m3i+cV/QIh9Fcgo8
R+snSlbOZMzCpUIvcuVkEMBP8+89/BtIabXL8SoTsD6v/f/YJfcw9qpOH+AoA3JG
```

UZT+0VxfIk0JUkX8QvM2qMQYY9efX+Dq+N0ODS1vsdP43pKxowOQlQUPKOsqoDch
IXW9qDD3uV+clg5L6BqDbX1O98oegcg6L24ZK1yKVzotiTj/eaZVpzTtrNYzWB0+
qO9FTwLqOmIRcduKKu5zctC7QlpFY3U2ikbkYpPsam/9GSXVe0LuMRLleiMPQUdU
ZJlkZr221OGq5TVhyJ6zEwud26wExB16tLU26ZvEFwExoUPboH/UQwX8L9vd8BKp
a32u35n5MOn+54Rfa4qfpU+uLB056CCKL8PwVLN9Xzeg+gJLfWqwEalPmSsylakO
7+suOGaUKy1a/uszD97dKk3Abwfoyb0qvbdF131GR04NYIzkQl72CBlxuWqVUt9o
pmwsUDAzwoJWi0sKy0dTm3KZHLJ+3OMIydod3beS9uS6Yro6NJBN5EPw3PoByBF5
DUkOfW6tV0dlHyXOuwU+JzBd4iwJgO53GVPAap8a/eOGgNCiw72gYM4lcHnwShL0
/v969VqntPXb7YF1hMs6ef3zTmLEB4xaXcARynnNkZnpQppxSPeHeXU+KxZCjkLE
brzHFnUMr8UJOyra3C/iXfi/OKJcBIURc3oY29Q45GBcV0s/W3n8TVF4qEqtbv3c
NbEmgcdzLGA28XiuyUH+pLxK3qP54jlqhd22q5qoN/gz4MKG+hJMMcO00Hj7+4Fb
fnxxGE5far3zjHLaxfnRKIfseU9DrQVh6gTg8ibe0kdoUXrptIb51eRcukE7s/yc
01Play8GYik4x+kcNAmQT29EslB/3RcrWH3tZExJjjDaC+Ty2atCMmlLGxt7VHOa
C3k0QHYSE/TULBldB64S1vVFrZgzLFTlXKGm38mOGCG3t/lQQDTo3IAp0YE+atM3
VG6ON3SSU0QRP1aEkZY8t9rf3+/J8Nl8oF4kF9ISzLNhlR/KJlNkmDvG/ic0skJK
KYezuuYH8/eEr9ZFfBsb9mRsFCM9iBZl/XqebCCC5/kfXzL/Hpp4f0L7DH4C0f6L
LbMCFhvsCNGh+1pdIjN9hbAkv/r2NN8+MaY2xFk0ukLfKgpLp0EfpkkcM0EZcvFn
j1JpB7rshCLj4PzM77fLh99H4cffL2qyzXqFF2Y7iW28bW/RQFxYwpyEnowrcRH/
11Qi525SdKWRkb9QlTJqFI6wsWe5kmYO/kDqGUpGPGK8+XTRTFjTci7NPLqN+s0w
Z4/b5SMVucBKq9sUm6g=
-----END
 ENCRYPTED PRIVATE KEY-----
Create NV seed_file
nv_seed_file_create:

Entropy write/update seed file
entropy_seed_file:"data_files/entropy_seed":0

Entropy write/update seed file
entropy_seed_file:"no_such_dir/file":MBEDTLS_ERR_ENTROPY_FILE_IO_ERROR

Entropy too many sources
entropy_too_many_sources:

Entropy output length #1
entropy_func_len:0:0

Entropy output length #2
entropy_func_len:1:0

Entropy output length #3
entropy_func_len:2:0

Entropy output length #4
entropy_func_len:31:0

Entropy output length #5
entropy_func_len:65:MBEDTLS_ERR_ENTROPY_SOURCE_FAILED

Entropy failing source
entropy_source_fail:"data_files/entropy_seed"

Entropy threshold #1
entropy_threshold:16:2:8

Entropy threshold #2
entropy_threshold:32:1:32

Entropy thershold #3
entropy_threshold:16:0:MBEDTLS_ERR_ENTROPY_SOURCE_FAILED

Entropy thershold #4
entropy_threshold:1024:1:MBEDTLS_ERR_ENTROPY_SOURCE_FAILED

Check NV seed standard IO
entropy_nv_seed_std_io:

Check NV seed manually #1
entropy_nv_seed:"00112233445566778899AABBCCDDEEFF00112233445566778899AABBCCDDEEFF0011223
3445566778899AABBCCDDEEFF00112233445566778899AABBCCDDEEFF"

Check
NV seed manually #2
entropy_nv_seed:"000000000

```
    <Configuration>Debug</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
    <Configuration>Release</Configuration>
    <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
    <Configuration>Release</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
</ItemGroup>
<ItemGroup>
  <ClCompile Include="..\..\programs\pkey\dh_client.c" />
</ItemGroup>
<ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">

    <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
</ItemGroup>
<PropertyGroup Label="Globals">
  <ProjectGuid>{4D29BE4A-979C-C5AE-44B5-30FB37D8D4EE}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>dh_client</RootNamespace>
</PropertyGroup>
<Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
    <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
```

```
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
/>
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
     <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
```

```
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
```

```
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
  </Link>
 </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
 <Import
 Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTIwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTMwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATrkzCJLznh
lhnsv1RXB9kfeaD+cIruPQ0cItBDGpdvD8xbBVvQci4+RG2RVUCSWRhkFYjSsUSM
0QHMQnBFlhw2o4GJMIGGMB0GA1UdDgQWBBTmVnUSF2MYwws/nCMv7b1wJVkDmjBX
BgNVHSMEUDBOgBTZTtbi+j0Sm/Zs/+gTkWdASpQzfqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTExggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgWsm+rHJgwUEyNm8EKbEds5yurpp5/3y5
PsvXJVDqxogCIQDUP0Jcl3A907CE2tPVXSgD6LQ6CPu19mixemPw60yijA==
-----END CERTIFICATE-----
CMAC self test
mbedtls_cmac_self_test:
```

CMAC null arguments
mbedtls_cmac_null_args:

CMAC init #1 AES-128: OK
depends_on:MBEDTLS_AES_C
mbedtls_cmac_setkey:MBEDTLS_CIPHER_AES_128_ECB:128:0

CMAC init #2 AES-192: OK
depends_on:MBEDTLS_AES_C
mbedtls_cmac_setkey:MBEDTLS_CIPHER_AES_192_ECB:192:0

CMAC init #3 AES-256: OK
depends_on:MBEDTLS_AES_C
mbedtls_cmac_setkey:MBEDTLS_CIPHER_AES_256_ECB:256:0

CMAC init #4 3DES : OK
depends_on:MBEDTLS_DES_C
mbedtls_cmac_setkey:MBEDTLS_CIPHER_DES_EDE3_ECB:192:0

CMAC init #5 AES-224: bad key size
depends_on:MBEDTLS_AES_C
mbedtls_cmac_setkey:MBEDTLS_CIPHER_ID_AES:224:MBEDTLS_ERR_CIPHER_BAD_INPUT_DATA

CMAC init #6 AES-0: bad key size
depends_on:MBEDTLS_AES_C
mbedtls_cmac_setkey:MBEDTLS_CIPHER_ID_AES:0:MBEDTLS_ERR_CIPHER_BAD_INPUT_DATA

CMAC init #7 Camellia: wrong cipher
depends_on:MBEDTLS_CAMELLIA_C
mbedtls_cmac_setkey:MBEDTLS_CIPHER_ID_CAMELLIA:128:MBEDTLS_ERR_CIPHER_BAD_INPUT_DA
TA

CMAC Single Blocks #1 - Empty block, no updates
mbedtls_cmac_multiple_blocks:MBEDTLS_CIPHER_AES_128_ECB:"2b7e151628aed2a6abf7158809cf4f3c":128
:16:"":-1:"":-1:"":-1:"":-1:"bb1d6929e95937287fa37d129b756746"

CMAC
Single Blocks #2 - Single 16 byte block
mbedtls_cmac_multiple_blocks:MBEDTLS_CIPHER_AES_128_ECB:"2b7e151628aed2a6abf7158809cf4f3c":128
:16:"6bc1bee22e409f96e93d7e117393172a":16:"":-1:"":-1:"":-1:"070a16b46b4d4144f79bdd9dd04a287c"

CMAC Single Blocks #3 - Single 64 byte block
mbedtls_cmac_multiple_blocks:MBEDTLS_CIPHER_AES_128_ECB:"2b7e151628aed2a6abf7158809cf4f3c":128
:16:"6bc1bee22e409f96e93d7e117393172aae2d8a571e03ac9c9eb76fac45af8e5130c81c46a35ce411e5fbc1191a0a52
eff69f2445df4f9b17ad2b417be66c3710":64:"":-1:"":-1:"":-1:"51f0bebf7e3b9d92fc49741779363cfe"

CMAC Multiple Blocks #1 - Multiple 8 byte blocks

mbedtls_cmac_multiple_blocks:MBEDTLS_CIPHER_AES_128_ECB:"2b7e151628aed2a6abf7158809cf4f3c":128
:16:"6bc1bee22e409f96":8:"e93d7e117393172a":8:"":-1:"":-1:"070a16b46b4d4144f79bdd9dd04a287c"

CMAC Multiple Blocks #2 - Multiple 16 byte blocks
mbedtls_cmac_multiple_blocks:MBEDTLS_CIPHER_AES_128_ECB:"2b7e151628aed2a6abf7158809cf4f3c":128
:16:"6bc1bee22e409f96e93d7e117393172a":16:"ae2d8a571e03ac9c9eb76fac45af8e51":16:"30c81c46a35ce411e5fb
c1191a0a52ef":16:"f69f2445df4f9b17ad2b417be66c3710":16:"51f0bebf7e3b9d92fc49741779363cfe"

CMAC
Multiple Blocks #3 - Multiple variable sized blocks
mbedtls_cmac_multiple_blocks:MBEDTLS_CIPHER_AES_128_ECB:"2b7e151628aed2a6abf7158809cf4f3c":128
:16:"6bc1bee22e409f96":8:"e93d7e117393172aae2d8a571e03ac9c":16:"9eb76fac45af8e5130c81c46a35ce411e5fbc
1191a0a52ef":24:"f69f2445df4f9b17ad2b417be66c3710":16:"51f0bebf7e3b9d92fc49741779363cfe"

CMAC Multiple Blocks #4 - Multiple 8 byte blocks with gaps
mbedtls_cmac_multiple_blocks:MBEDTLS_CIPHER_AES_128_ECB:"2b7e151628aed2a6abf7158809cf4f3c":128
:16:"":0:"6bc1bee22e409f96":8:"":0:"e93d7e117393172a":8:"070a16b46b4d4144f79bdd9dd04a287c"

CMAC Multiple Operations, same key #1 - Empty, empty
mbedtls_cmac_multiple_operations_same_key:MBEDTLS_CIPHER_AES_192_ECB:"8e73b0f7da0e6452c810f32b
809079e562f8ead2522c6b7b":192:16:"":-1:"":-1:"":-1:"d17ddf46adaacde531cac483de7a9367":"":-1:"":-1:"":-
1:"d17ddf46adaacde531cac483de7a9367"

CMAC
Multiple Operations, same key #2 - Empty, 64 byte block
mbedtls_cmac_multiple_operations_same_key:MBEDTLS_CIPHER_AES_192_ECB:"8e73b0f7da0e6452c810f32b
809079e562f8ead2522c6b7b":192:16:"":-1:"":-1:"":-
1:"d17ddf46adaacde531cac483de7a9367":"6bc1bee22e409f96e93d7e117393172aae2d8a571e03ac9c9eb76fac45af8
e5130c81c46a35ce411e5fbc1191a0a52eff69f2445df4f9b17ad2b417be66c3710":64:"":-1:"":-
1:"a1d5df0eed790f794d77589659f39a11"

CMAC Multiple Operations, same key #3 - variable byte blocks
mbedtls_cmac_multiple_operations_same_key:MBEDTLS_CIPHER_AES_192_ECB:"8e73b0f7da0e6452c810f32b
809079e562f8ead2522c6b7b":192:16:"6bc1bee22e409f96e93d7e117393172aae2d8a571e03ac9c9eb76fac45af8e51"
:32:"30c81c46a35ce411e5fbc1191a0a52eff69f2445df4f9b17ad2b417be66c3710":32:"":-
1:"a1d5df0eed790f794d77589659f39a11":"6bc1bee22e409f96e93d7e117393172aae2d8a571e03ac9c9eb76fac45af8
e51":32:"30c81c46a35ce411e5fbc1191a0a52eff69f2445df4f9b17ad2b417be66c3710":32:"":-
1:"a1d5df0eed790f794d77589659f39a11"
-----BEGIN EC PRIVATE KEY-----
MF8CAQEEGDOOhqiB4jj1Sb1vBVNJS3Pj1hEw/cbJbaAKBggqhkjOPQMBAaE0AzIA
BFF1vN8wo3DznVOT5hJyiNgBZ7X0tLd2xnT3xvNUt9IkBiwfaFS1p68P5Xjq8ljw
Jw==
-----END EC PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTcwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTgwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASsc/JkNcYf

bMgpOfrL5kKOGxOJaGS6SQIeNO33UeBpToe1bU2acN652xjvcGo0fJEtxg2fcPHR
hTnGMBD1u1N2o4GJMIGGMB0GA1UdDgQWBBSDbIpYntlhJ0GgIsyd75XRhlC18jBX
BgNVHSMEUDBOgBSnjWvpWxZcFnfQ2KGtCg/u6fT/D6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTE2ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAJo2NXfJU1sK6SVTu4OV21FKITlXntMi
oenYMsBjzO8oAiEAidSELcLjjAHi3mfBARvCgKlRhmbNEMCHQT7Ha7ZQoRw=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTYwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTcwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAARrISq2zO9m
D29YCLHB56FdU/RINtRhfeLtM+u5o3HaAnopy0S98RzuEGELjpzr8ZI6kkMMZsj8
nFZQF8HfuE0go4GJMIGGMB0GA1UdDgQWBBSnjWvpWxZcFnfQ2KGtCg/u6fT/DzBX
BgNVHSMEUDBOgBRTw3K0Psy3u/6+3KKSoaQqJnPvPqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTE1ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgDgXjoc6FfMF5W0NziV6vx2BOPNWav01Z
ynEP4h9ULnUCIQC1rU4sEId3UdjzTKhpSGTKtaOuPG+b0YdEMPimI4jmVw==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTUwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTYwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQ7Vsp7JmDN
kgPh/+zmIPkd7o0xot/WPMFn3uAsGtsU385MF0fmhfFLhRbbH9h4JjYHj8y0spU3
buUXhftvAZVbo4GJMIGGMB0GA1UdDgQWBBRTw3K0Psy3u/6+3KKSoaQqJnPvPjBX
BgNVHSMEUDBOgBR1mXlrdW5rx1VnqMMnUBXo0WWGWqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTE0ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAMJnGjE9v3SjuGfi0jNByrwyNfhlTHMh
FhPQidNrDpXwAiEAqYtNiV8t9RrAa9GC6FWDuJpvIiU6FsE+lFq6uIq/J2E=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTQwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTUwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQlKUiMoSss
/hsTasedqdB2BCOGJhTt0hgUGeUnWNZ1svO4yn0GkFHZ08++fl2MKqjpj+VXq0JS
FFyGUOgmgi3Ho4GJMIGGMB0GA1UdDgQWBBR1mXlrdW5rx1VnqMMnUBXo0WWGWjBX
BgNVHSMEUDBOgBRNsJB++ccSBmbCCKBxi4CjXROBk6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTEzggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAKYOIo+fdCQRqpH4LN8qUK1aKzKmWGxS
fGzEEkg/29bMAiAl95cmucoCDMq2Ab8Coc0dEqyJ6+rAPMLBCbGawyiW6A==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTMwHhcNMTcwNjIyMTE1MDMzWhcN

MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTQwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATRMZN0RHzP
donNmZuq9XPhzvQ52TaokxT39qpQtlFyvUuEGKrLoNvdcpARaA0rGput6RLAQOVU
iNVlJ3Ipj789o4GJMIGGMB0GA1UdDgQWBBRNsJB++ccSBmbCCKBxi4CjXROBkzBX
BgNVHSMEUDBOgBTmVnUSF2MYwws/nCMv7b1wJVkDmqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTEyggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgVfuLpjp08AaxKWf6cuZUUCRd7CojSS1I
71hzeUyFS+sCIQDNJI6P/pBbiHgTaGlBAgfcEfmxmbY0n4xZndtxIkmyVA==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTIwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTMwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATrkzCJLznh
lhnsv1RXB9kfeaD+cIruPQ0cItBDGpdvD8xbBVvQci4+RG2RVUCSWRhkFYjSsUSM
0QHMQnBFlhw2o4GJMIGGMB0GA1UdDgQWBBTmVnUSF2MYwws/nCMv7b1wJVkDmjBX
BgNVHSMEUDBOgBTZTtbi+j0Sm/Zs/+gTkWdASpQzfqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTExggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgWsm+rHJgwUEyNm8EKbEds5yurpp5/3y5
PsvXJVDqxogCIQDUP0Jcl3A907CE2tPVXSgD6LQ6CPu19mixemPw60yijA==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTEwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTIwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATDE9LPlLPc
gZ3b0BchR/AkhNEP9HAavwYadJIyzoPo5edCVnboQH786jsZwZNZoC0gHDAhCmGc
IfRenISAoVuPo4GJMIGGMB0GA1UdDgQWBBTZTtbi+j0Sm/Zs/+gTkWdASpQzfjBX
BgNVHSMEUDBOgBSOSt6ePyMRT6PGMaIi7FqNX9MKtKEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTEwggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgYYF5AnRV7eh2hLD5Dz//pceMTKz9Ls46
E6DxvbfDHikCIFttlGrOCZVyS4ocsjuKIELVUX5qfygI0sn4kU3qCTs2
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTAwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATZwR+WK6NB
F/7riFdN63c8hjYddZRR4lrzVNPwiBQxnnxwpPyrD9A6aPPmLc6SqGOJW4ZGVCco
IBze9RJVeiB9o4GJMIGGMB0GA1UdDgQWBBSOSt6ePyMRT6PGMaIi7FqNX9MKtDBX
BgNVHSMEUDBOgBQtxZSLJAkEz+2RKMQexM6EtsfgcqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA5ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgN//NqM0FrkrMjmxoeCY9DgxkH2R6sQ4d
NgtwCZAIqEICIBs4vupaVcuvni9tltbP26wi7c0FR+blZuo5DPIA3SVe
-----END

CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDkwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTAwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAR6jlGKbJd5
hiDxN789gkOcwpyHI9wRwCrADAOwOkMePBPRlwGdm7mw7Z/EAmu26zRm/hcyrs4M
qk2LabDjPI9Xo4GJMIGGMB0GA1UdDgQWBBQtxZSLJAkEz+2RKMQexM6EtsfgcjBX
BgNVHSMEUDBOgBT6gyXHzPIPYc1Vr1aGiLLeMh4HpqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA4ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgP7S8vFstfUBdNe6ym5GYG5Q+aBVEKqRs
fVW7HNUktSYCIQDo6Jua6o/DJbrpq4qYWq5gv4yGyzPTN+3IaKrEICdaaw==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDgwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDkwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAR7ZB16+t6E
sfahGyKUGJW5mezkzjdaYvc4lbJaKNRwFRfc3F/fmNOSsUFSg/F0N+vUE+doKiPC
8wRwLzvm4s+5o4GJMIGGMB0GA1UdDgQWBBT6gyXHzPIPYc1Vr1aGiLLeMh4HpjBX
BgNVHSMEUDBOgBS40mLt93U8Sh8ZGiDVAhRSiBPcXqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA3ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgO4el1ZPhlIli/qNR2SIEiuvs5Mmy868i
N2Rv5X/VxIECIA/8rUALQxW38XSdBVX3e/jzu7ju47n1YwEqD9K9WdVv
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDcwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDgwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAARpQeQ/YGQj
nl7Szo6WStJ1u7xunTL5jBkXH8aAVSm0qiX4AD/7YPxa5EnGzZdLTn25vQVnfQAG
pMx8P1lYiGYCo4GJMIGGMB0GA1UdDgQWBBS40mLt93U8Sh8ZGiDVAhRSiBPcXjBX
BgNVHSMEUDBOgBREq5J3toJPxZ3O+ssJ5vkkU0RJE6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA2ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhANwGf+F4a+kmXWz8UjSpRkaToTV6EFWw
/Tjzj0tQhDoAAiEA19RxeWOVBBpM6LOHg6v5Lf54YN1snkLf+sEXyZCuWQQ=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDYwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDcwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASNOj4d4MEA
7p/3miijqG4ToE4opKPAm+3BTIGrJTYT14++TSiUICl0ASXj+xeUcLMIaXTN042s
LsHxpShzQaL0o4GJMIGGMB0GA1UdDgQWBBREq5J3toJPxZ3O+ssJ5vkkU0RJEzBX
BgNVHSMEUDBOgBSjovYaC/m6Li9Tp0V9iZRs9267Q6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA1ggEBMAwGA1UdEwQF

MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAKGcf+c442c/XiwubbaiQvsoZ7EoVxuM
oKmia0gPyBNkAiEA83asjJ5FDXQuLyZpczviXrbmqgCPOfYadtvkc0cxMis=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDUwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDYwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASA9qWoAUHr
nn+3kxyNrjPJk82WDLimW21RN51uxpobadv8YgGEDRdP+Ok+uRqQSUsA6ZXfF3iG
r2GjfQ3wMDH8o4GJMIGGMB0GA1UdDgQWBBSjovYaC/m6Li9Tp0V9iZRs9267QzBX
BgNVHSMEUDBOgBTXh06MAV9S4l4lG1TKOrKRBh4qn6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA0ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgcjZNFWJtlDmoPZbAxqsGczRYK0lfPgu6
g1H7pp0ce+wCIDj9BRZM2OB9EF0e+MDKGjyZGfvfrL6Ir47x/KrM6H8T
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDQwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDUwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQEdT0OFf5G
UcrgX2XllCyJzP94NZ464GsgB6psNLsDeL+j7AU+oJy7VLvW/lHh3ODgl08Z9bhq
LFBmNjnHbm8Qo4GJMIGGMB0GA1UdDgQWBBTXh06MAV9S4l4lG1TKOrKRBh4qnzBX
BgNVHSMEUDBOgBQox4F1NsZunlsduoGvzIgRSYfB36EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAzggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAIW++zqDZlLLUk/emePohdNOp5JO3wS9
XvkBJ6Wua7GBAiAdx+EKmdjVrwnzrQltTgnmSfGMXhKNYifK3uD83W3pcQ==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDMwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDQwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQUXDgcUVNT
9hovbZE5HL6rjOb7C55wEuWKThV/CcZ4rWrXx7VXHYdD/R3aDA7JSvYpm2sTok4i
sblDzhZM/GDNo4GJMIGGMB0GA1UdDgQWBBQox4F1NsZunlsduoGvzIgRSYfB3zBX
BgNVHSMEUDBOgBQApzZdtBdD3dLxouQpr/aDiVttd6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAyggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgAkiNhqFAZXSUWEDK91OZvQGdeZOtd6mC
+Wv3fGk3t28CIEKOwidkUTUaiPdZ4efmAr+CEeGzdq27ob2S+nqqHqgV
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDIwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDMwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQRDXDNIi1p
ereudhqwa2LslXgsxnB63Hu5y5lg+1WPruIYPzD/Ho0APveVdzFLVji19+bE4+tF

PYL1SpsN1WfWo4GJMIGGMB0GA1UdDgQWBBQApzZdtBdD3dLxouQpr/aDiVttdzBX
BgNVHSMEUDBOgBT5RCgQ0AlZTQbfFB2+6+w0XRvydaEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAxggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAOnd+7bAofkHVa4KFNjv3TCegw1lrhuM
8Of8wgvrTEGoAiEAsS8iKMpSfXH4D0egg4gLamE6akde965rDtySU+ve9lg=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDEwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDIwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQWHpv1i6lf
wvNPOP5ka6S0n55EvzoaYK6pbTXP6yMOW/4XZSPKx5Zoq4FMe0cKzGIIFL1rzj1V
2czYB+qvLhyio4GJMIGGMB0GA1UdDgQWBBT5RCgQ0AlZTQbfFB2+6+w0XRvydTBX
BgNVHSMEUDBOgBSh3uHkX5nj86yFEFwjscSWM40P+qEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAI7unGW/gr9tOc3i+dF5N815srgh+FrX
oj9Et74EcSpTAiBubv+vOH0DE0gmYI11HeAIgutWqqMIC72dZlwTF/Vi3g==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB3jCCAYWgAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDAwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQznn9zHHwL
GO8VR4W9V7vMlxCdoojzEOiX5Y6JtPtFOz866ueHY6zoN0/mJ6DnqnSXilJIUUeW
6eGfqmka7nxko4GRMIGOMB0GA1UdDgQWBBSh3uHkX5nj86yFEFwjscSWM40P+jBf
BgNVHSMEWDBWgBQlFYvU5WboI4fcdPoiQs8/fPHZraEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggkA/KCWhcqToHAw
DAYDVR0TBAUwAwEB/zAKBggqhkjOPQQDAgNHADBEAiBasbuinP+pJTU4oDCVD8zQ
1rJBDSOKIEyWu84/D6Hj6wIgVMPUoO01bPhzllAa/gW8Xk/daey09SBgN3AT9pWU
TDA=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIBpTCCAUugAwIBAgIJAPygloXKk6BwMAoGCCqGSM49BAMCMC8xCzAJBgNVBAYT
AlVLMREwDwYDVQQKDAhtYmVkIFRMUzENMAsGA1UEAwwEQ0EwMDAeFw0xNzA2MjIx
MTUwMzJaFw0yNzA2MjMxMTUwMzJaMC8xCzAJBgNVBAYTAlVLMREwDwYDVQQKDAht
YmVkIFRMUzENMAsGA1UEAwwEQ0EwMDBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IA
BFW41/qAwAPpy+Txdc7PKmzZsq9CPiujKU4vpF1ekXnGx2HP420QobwBVVWhkzRm
LwdboH2j65dcCKjQ7mv/dxKjUDBOMB0GA1UdDgQWBBQlFYvU5WboI4fcdPoiQs8/
fPHZrTAfBgNVHSMEGDAWgBQlFYvU5WboI4fcdPoiQs8/fPHZrTAMBgNVHRMEBTAD
AQH/MAoGCCqGSM49BAMCA0gAMEUCIQC7iRcVzwMyfVK5imirJ7MqJQ04euH4CLOt
IZ+SNfaERAIgSU0MWFDosVEIpg8YMqIHeF7Mg4ZyH6+fGazJgVLttUY=
-----END
CERTIFICATE-----
-----BEGIN X509 CRL-----
MIIBqzCBlDANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDERMA8GA1UEChMI
UG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EXDTExMDIyMDEwMjQx

OVoXDTExMDIyMDExMjQxOVowKDASAgEBFw0xMTAyMTIxNDQ0MDdaMBICAQMXDTEx
MDIxMjE0NDQwN1owDQYJKoZIhvcNAQEFBQADggEBAKgP1XmCIPbfY1/UO+SVFQir
jArZ94QnQdoan4tJ29d8DmTxJ+z9/KyWNoGeOwc9P/2GQQaZahQOBr0f6lYd67Ct
wFVh/Q2zF8FgRcrQV7u/vJM33Q2yEsQkMGlM7rE5lC972vUKWu/NKq8bN9W/tWxZ
SFbvTXpv024aI0IRudpOCALnIy8SFhVb2/52IN2uR6qrFizDexMEdSckgpHuJzGS
IiANhIMn5LdQYJFjPgBzQU12tDdgzcpxtGhT10y4uQre+UbSjw+iVyml3issw59k
OSmkWFb06LamRC215JAMok3YQO5RnxCR8EjqPcJr+7+O9a1O1++yiaitg4bUjEA=
-----END X509 CRL-----
-----BEGIN X509 CRL-----
MIIBcTCB9wIBATAKBggqhkjOPQQDAjA+MQswCQYDVQQGEwJOTDERMA8GA1UEChMI
UG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EXDTEzMDkyNDE2
MzEwOFoXDTIzMDkyMjE2MzEwOFowFDASAgEKFw0xMzA5MjQxNjI4MzhaoHIwcDBu
BgNVHSMEZzBlgBSdbSAkSQE/K8t4tRm8fiTJ2/s2fKFCpEAwPjELMAkGA1UEBhMC
TkwxETAPBgNVBAoTCFBvbGFyU1NMMRwwGgYDVQQDExNQb2xhcnNzbCBUZXN0IEVD
IENBggkAwUPifmJDzOgwCgYIKoZIzj0EAwIDaQAwZgIxAKuQ684s7gyhtxKJr6Ln
S2BQ02f1jjPHrZVdXaZvm3C5tGi2cKkoK1aMiyC3LsRCuAIxAIMhj0TmcuIZr5fX
g5RByD7zUnZBpoEAdgxFy4JPJ2IViWOPekSGh8b/JY1VNS6Zbw==
-----END
X509 CRL-----
Single low error
depends_on:MBEDTLS_AES_C
error_strerror:-0x0020:"AES - Invalid key length"

Single high error
depends_on:MBEDTLS_RSA_C
error_strerror:-0x4080:"RSA - Bad input parameters to function"

Low and high error
depends_on:MBEDTLS_AES_C:MBEDTLS_RSA_C
error_strerror:-0x40A0:"RSA - Bad input parameters to function \: AES - Invalid key length"

Non existing high error
error_strerror:-0x8880:"UNKNOWN ERROR CODE (8880)"

Non existing low error
error_strerror:-0x007F:"UNKNOWN ERROR CODE (007F)"

Non existing low and high error
error_strerror:-0x88FF:"UNKNOWN ERROR CODE (8880) \: UNKNOWN ERROR CODE (007F)"
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">

```
    <Configuration>Debug</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
    <Configuration>Release</Configuration>
    <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
    <Configuration>Release</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
</ItemGroup>
<ItemGroup>
  <ClCompile Include="..\..\programs\ssl\ssl_client2.c" />
</ItemGroup>
<ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">

    <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
</ItemGroup>
<PropertyGroup Label="Globals">
  <ProjectGuid>{4E590E9D-E28F-87FF-385B-D58736388231}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>ssl_client2</RootNamespace>
</PropertyGroup>
<Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
```

```
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
/>
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
     <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
```

```
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
```

<GenerateDebugInformation>true</GenerateDebugInformation>
<EnableCOMDATFolding>true</EnableCOMDATFolding>
<OptimizeReferences>true</OptimizeReferences>
<AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
</Link>
</ItemDefinitionGroup>
<ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
<ClCompile>
<WarningLevel>Level3</WarningLevel>
<PrecompiledHeader>
</PrecompiledHeader>
<Optimization>MaxSpeed</Optimization>
<FunctionLevelLinking>true</FunctionLevelLinking>
<IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
<AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
</ClCompile>
<Link>
<SubSystem>Console</SubSystem>
<GenerateDebugInformation>true</GenerateDebugInformation>
<EnableCOMDATFolding>true</EnableCOMDATFolding>
<OptimizeReferences>true</OptimizeReferences>
<AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
</Link>
</ItemDefinitionGroup>
<Import
Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
<ImportGroup Label="ExtensionTargets">
</ImportGroup>
</Project>
-----BEGIN X509 CRL-----
MIIBcDCB9wIBATAKBggqhkjOPQQDAzA+MQswCQYDVQQGEwJOTDERMA8GA1UEChMI
UG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EXDTEzMDkyNDE2
MzEwOFoXDTIzMDkyMjE2MzEwOFowFDASAgEKFw0xMzA5MjQxNjI4MzhaoHIwcDBu
BgNVHSMEZzBlgBSdbSAkSQE/K8t4tRm8fiTJ2/s2fKFCpEAwPjELMAkGA1UEBhMC
TkwxETAPBgNVBAoTCFBvbGFyU1NMMRwwGgYDVQQDExNQb2xhcnNzbCBUZXN0IEVD
IENBggkAwUPifmJDzOgwCgYIKoZIzj0EAwMDaAAwZQIwateJaD13+Yi4HWBIlOov
8ZDsvnfQfW/R0A1s2ZccAi+byurShuNGiSvsFSh5d/6QAjEA427F8bNk/fdj5YXu
Oo1qEd7WpD2dNUb0draGSIcJGBRGzi5it14UXr9cR4S5eJ6Q
-----END X509 CRL-----
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
<ItemGroup Label="ProjectConfigurations">

```
  <ProjectConfiguration Include="Debug|Win32">
    <Configuration>Debug</Configuration>
    <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
    <Configuration>Debug</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
    <Configuration>Release</Configuration>
    <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
    <Configuration>Release</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
</ItemGroup>
<ItemGroup>
  <ClCompile Include="..\..\programs\x509\cert_req.c" />
</ItemGroup>
<ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">

  <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
</ItemGroup>
<PropertyGroup Label="Globals">
  <ProjectGuid>{C9E2AB15-8AEF-DD48-60C3-557ECC5215BE}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>cert_req</RootNamespace>
</PropertyGroup>
<Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
```

```
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
/>
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
   <PrecompiledHeader>
   </PrecompiledHeader>
```

```
    <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
     <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
   </Link>
   <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
   </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
   <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
   </Link>
   <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
   </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
```

<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
<AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
</ClCompile>
<Link>
<SubSystem>Console</SubSystem>
<GenerateDebugInformation>true</GenerateDebugInformation>
<EnableCOMDATFolding>true</EnableCOMDATFolding>
<OptimizeReferences>true</OptimizeReferences>
<AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
</Link>
</ItemDefinitionGroup>
<ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
<ClCompile>
<WarningLevel>Level3</WarningLevel>
<PrecompiledHeader>
</PrecompiledHeader>
<Optimization>MaxSpeed</Optimization>
<FunctionLevelLinking>true</FunctionLevelLinking>
<IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
<AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
</ClCompile>
<Link>
<SubSystem>Console</SubSystem>
<GenerateDebugInformation>true</GenerateDebugInformation>
<EnableCOMDATFolding>true</EnableCOMDATFolding>
<OptimizeReferences>true</OptimizeReferences>
<AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
</Link>
</ItemDefinitionGroup>
<Import
Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
<ImportGroup Label="ExtensionTargets">
</ImportGroup>
</Project>
-----BEGIN CERTIFICATE REQUEST-----
MIIBzTCCAQYCAQAwNDELMAkGA1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NMMRIw
EAYDVQQDEwlsb2NhbGhvc3QwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAN0R
ip+ZurBoyirqO2ptWZftTslU5A3uzqB9oB6q6A7CuxNA24oSjokTJKXF9frY9ZDX
yMrLxf6THa/aEiNzUnlGGrqgVyt2FjGzqK/nOJsIi2OZOgol7kXSGFi6uZMa7dRY
mmMbN/z3FAifhWVJ81kybdHg6G3eUu1mtKkL2kCVAgMBAAGgKTAnBgkqhkiG9w0B
CQ4xGjAYMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgXgMD0GCSqGSIb3DQEBCjAwoA0w
CwYJYIZIAWUDBAIDoRowGAYJKoZIhvcNAQEIMAsGCWCGSAFlAwQCA6IDAgE+A4GB
ACxWBhPkhyVlBY/mwkrW7OjYsaN2/ZlFSv76w63b61BpigReJsggMut5EPOgfGYJ

rzygKDlF/NtmMN22jWrFup9LsZJAX0gYbLmliiaG9Hch+i/8b42oaQTDWGFZ9LiY
W7F7X0f9lpzNKOtQ8ix0s+nYS2ONyzfu55+Rlzf8/63M
-----END CERTIFICATE REQUEST-----
-----BEGIN EC PRIVATE KEY-----
MIGkAgEBBDAtxOHUV4be1MdH1frBHzxITCyUSxrVjJN8QTvTVk558ka0a3zhd4Pb
ekWt7wBPXQegBwYFK4EEACKhZANiAATw6KHd9flIt43V2YWdxCVYzD35jqxduWGW
tcHGFfGPB3CkIcQ2f5+hRV2uphVhrtK6/dBV47qcnX0fdA2LFbyKTU/6HGxtqrxu
1rvy8DIeYLgSZdAuDXDujFv1DzapfVg=
-----END EC PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDFzCCAf+gAwIBAgIBATANBgkqhkiG9w0BAQsFADAmMSQwIgYDVQQDExtUZXN0
IGludGVybWVkaWF0ZSBtYXhwYXRoIDIwHhcNMDEwMTAxMDAwMDAwWhcNMzAxMjMx
MjM1OTU5WjAmMSQwIgYDVQQDExtUZXN0IGludGVybWVkaWF0ZSBtYXhwYXRoIDMw
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCRKuBYUPiVhDREX/PeYlmO
fWWA0GSGcI/SFyIm/962gw3dsIH65zx+jTDENDZlxvNMBDSoE2eMm8AnWqyVkD1u
ggEqZPwlKLGKL/VdMNYjcTlo69fWHqVbrqlWwjMubQ0B/RUmfbEvDRi/yF8pvCNw
14B+bsYLAkHyySN6Qwonz57qk/hkfGauc6jSRSUKDzDxErNnqxgnFfURN6RY8RRJ
euxxD9hKOk7OMsOmHWU7iBUSsGF0mAmknOeqStEGJHt/+EiukBXfA5Ru1+vGshvk
Vc4z2u3+y9ZFGvMhQacG+jThZn4pAc+wyf73HyL7+2546DUot+zXSFbRFaxNCOY5
AgMBAAGjUDBOMAwGA1UdEwQFMAMBAQEwHQYDVR0OBBYEFI4GvVTiHk9jI6oZ7+Am
DBaTsV97MB8GA1UdIwQYMBaAFMI3a8MtjW1x6dPPJGaVLhMF7bGKMA0GCSqGSIb3
DQEBCwUAA4IBAQCB3dtsoVdschVyCWSI16Se46RZJtLW1bM019KdyZj9DdIZ2VPm
Ip+BQFcVJyzbfmhn5QBbhNDKkwsfldI9Y8IqZ132j442/XIFZIilaPi3cE/WLFUY
Nxu2opuN3+KDwDYO32CUp3frr9OjAtB5amZnkXau+C1EkJlSuWaT+/gIlYwlr4/H
uADcyqFSmy28P9jmkK8AzZHhKnlRadAn2cDB8MFXD5VxnLJfejkprQVLdxTXRovP
cE/6c7PUGIK22WcSX8KTfuviKmjdGVhgeKps2nRNKaSIlqYCztyc8IjcZwJCnh6c
ZW8V9bi7WxDK+I9PPgrgLK8W+VTkS0RtjP5a
-----END
CERTIFICATE-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIEQZG5j8IkRLxa9OoZJzD3KkrXqIgi9cHZMVv2s/VcPOoAoGCCqGSM49
AwEHoUQDQgAEgVkxdkkk+hWtq6Axbg7tMxH6kSVVwbDBnANyPpi6LaRyN4kfQzeN
H4462PBX6C9PyQCk99tzD7LGBJTRQDs44w==
-----END EC PRIVATE KEY-----
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAq9eMvlV9hzsP+2u6oSlhxly+VSGe4I0Mly1gMku+BhiPm7EP
EscFe+cQcuA7kr6Wmzjan6v913igTri21Gh5llS+v7t4GdbfmfQSk8AiT0bC76+D
sZ/GaJ+AhHyFmc5CS3Y6O++kKE8LG9RqKW0HjnQjOH6YQr+FgWv7smU2fFHVdCVt
vIMzsRy3UfBhy5LcwGUGqrTjwn7QoSRBcgJKMp4cWBr14MKr4nJ+p7lu3QrfSGXU
3TXrgHtqiHTwSiaZ75pK4CzP4ywnebsA7YNRh2sPGWuTLVCu9FZZ9fR3x2NMz64d
OjUO+JEzqj34/0N+gV3nf9nQqbTexUtBa9SuEQIDAQABAoIBAHnxtYvgCPttG1NU
yJTTU/I7IEozWJaLIZMqfShT/Z4/0bEvfb3ag/bAKzkKDNx+6Utvlh1XJQTCMiiL
BhtHpHjc3JwdAgZ8KCMNRB2ba/2L/ouupqrm8hqOjdn2r6xM5Vi9pmegEIMWTJDM
NSX+nC0oF1Jg69X6KViFc5DOKFMhacSEwLJkv/EqCgdWaBoqMlTtTWKdm34xSN2L
P5o9kOgihTBNUUnVBUWJiT7C6bBAFwb1rECpvNOk6h+lvG+fSDZKYdwBrAsKspIy
/aXZD4qaicefGblrHcZv2og/zYkFs4riWNOmglxZyrK/3rFFk0B8mBk1mWQvrK7+
Jq/R4k0CgYEA0hO29hJjeTBDdOWgzyXr5uppmR1WU7fv/Jy8PLRMvUvmiMQqRDK3
zwGc6H938wdsubpdTCLPhq0rhDCTqtwIEAuFjZIYJs4yZzfy6klaD3516iIgb+W7

fe1RkYMBp9wV0x272vzP4Y5p/fzp5xhvN52OkhQsjHRHewfDaUwSFScCgYEA0Wgi
kGVK6OxzoMCgiWx/L+y3yrYuHdWANTIIa5RvZk4UQqEFkGYGVP1rpbB/fAa1Yqev
qXkLZqad2dhJCuBVryGt29CHsbnEQ/QuTwlGmyZj1U8NnJBgNCPTdmGTBIm/7w9S
ESZ48bUlcqzsZn1Big/A6JX1e5i9b/1jyozNVgcCgYEAnRZc49iQRZjPeGQVQZEL
u5ph6DrFyMhsTistnv77uzk8Y9y79k8unz6HhFt86GAO7zrqdPo60GxBdBGW+laa
ONVEwr4SDUJ28jQmEwdSru9TYQav1ryk3N9O9U5POKQcNcewJ2qQUAvcOi6bAVGG
KMJKT/WB8m0o3ljJyL03cFUCgYBoHFTq42Fd8oj+SCbIjCej5RXvc6nz7Tzjta9Y
BSFphLIv+ixxAThustv9MYYAXLl7hhEgueyAKaBbOVv/S09uVdlBayi7pLc+bb1E
UEFJS8nguH/08hbSdWlh9tsIK5BAQ6ayniUNTtmCbRTPU8Ds6i4ntL6qp2KvthQS
FPTVqwKBgQC8m2sJapMms0/7EeGpUwMO+WNCHeRyujnriWYL8Kms0lmAn8NrQoA5
wgbx0nZ/VrXtLPGHy915jxDXOU1Yc2gqEf5Qm/GnByUuml1mUSldiPciSJvKzMqP
LeWnb62HD60t/zwstN20Yzt6mBLocm1PPdPhPweI/EF6pSgvlw5NTw==
-----END
RSA PRIVATE KEY-----
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
<ItemGroup Label="ProjectConfigurations">
<ProjectConfiguration Include="Debug|Win32">
<Configuration>Debug</Configuration>
<Platform>Win32</Platform>
</ProjectConfiguration>
<ProjectConfiguration Include="Debug|x64">
<Configuration>Debug</Configuration>
<Platform>x64</Platform>
</ProjectConfiguration>
<ProjectConfiguration Include="Release|Win32">
<Configuration>Release</Configuration>
<Platform>Win32</Platform>
</ProjectConfiguration>
<ProjectConfiguration Include="Release|x64">
<Configuration>Release</Configuration>
<Platform>x64</Platform>
</ProjectConfiguration>
</ItemGroup>
<ItemGroup>
<ClCompile Include="..\..\programs\pkey\pk_encrypt.c" />
</ItemGroup>
<ItemGroup>
<ProjectReference Include="mbedTLS.vcxproj">

<Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
</ProjectReference>
</ItemGroup>
<PropertyGroup Label="Globals">
<ProjectGuid>{55007179-7746-9CFB-97EC-65102FB272C8}</ProjectGuid>
<Keyword>Win32Proj</Keyword>
<RootNamespace>pk_encrypt</RootNamespace>

```
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
   <UseDebugLibraries>true</UseDebugLibraries>
   <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
   <UseDebugLibraries>true</UseDebugLibraries>
   <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
    <ConfigurationType>Application</ConfigurationType>
   <UseDebugLibraries>false</UseDebugLibraries>
   <WholeProgramOptimization>true</WholeProgramOptimization>
   <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
   <UseDebugLibraries>false</UseDebugLibraries>
   <WholeProgramOptimization>true</WholeProgramOptimization>
   <CharacterSet>Unicode</CharacterSet>
   <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
 />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
```

```
    <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
  </PropertyGroup>
  <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
   <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
  </PropertyGroup>
  <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <LinkIncremental>false</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
  </PropertyGroup>
  <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
   <LinkIncremental>false</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
  </PropertyGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
     <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
   </Link>
   <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
   </ProjectReference>
  </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
   <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
    <SubSystem>Console</SubSystem>
```

```
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
```

```
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
 <Import
 Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
-----BEGIN X509 CRL-----
MIICejCCATECAQEwPgYJKoZIhvcNAQEKMDGgDTALBglghkgBZQMEAgOhGjAYBgkq
hkiG9w0BAQgwCwYJYIZIAWUDBAIDogQCAgC+MDsxCzAJBgNVBAYTAk5MMREwDwYD
VQQKEwhQb2xhclNTTDEZMBcGA1UEAxMQUG9sYXJTU0wgVGVzdCBDQRcNMTQwMTIw
MTM1NjM4WhcNMjQwMTE4MTM1NjM4WjAoMBICAQoXDTEzMDkyNDE2MjgzOFowEgIB
FhcNMTQwMTIwMTM0MzA1WqBnMGUwYwYDVR0jBFwwWoAUtFrkpbPe0lL2udWmlQ/r
PrzH/f+hP6Q9MDsxCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEZMBcG
A1UEAxMQUG9sYXJTU0wgVGVzdCBDQYIBADA+BgkqhkiG9w0BAQowMaANMAsGCWCG
SAFlAwQCA6EaMBgGCSqGSIb3DQEBCDALBglghkgBZQMEAgOiBAICAL4DggEBAB9F
ywBfxOjetxNbCFhOYoPY2jvFCFVdlowMGuxEhX/LktqiBXqRc2r5naQSzuHqO8Iq
1zACtiDLri0CvgSHlravBNeY4c2wj//ueFE89tY5pK9E6vZp7cV+RfMx2YfGPAA2
t7tWZ2rJWzELg8cZ8hpjSwFH7JmgJzjE5gi2gADhBYO6Vv5S3SOgqNjiN1OM31AU
p6GHK5Y1jurF5Zwzs+w3wXoXgpOxxwEC4eiS86c9kNSudwTLvDTU0bYEQE1cF+K0
sB8QWABFJfuO5kjD2w3rWgmAiOKsZoxd1xrda+WD3JhDXnoVq3oVBIVlWVz6YID8
enMfMvwScA5AImzu9xA=
-----END X509 CRL-----
-----BEGIN CERTIFICATE-----
MIIB3jCCAYWgAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDAwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQznn9zHHwL
GO8VR4W9V7vMlxCdoojzEOiX5Y6JtPtFOz866ueHY6zoN0/mJ6DnqnSXilJIUUeW
6eGfqmka7nxko4GRMIGOMB0GA1UdDgQWBBSh3uHkX5nj86yFEFwjscSWM40P+jBf
BgNVHSMEWDBWgBQlFYvU5WboI4fcdPoiQs8/fPHZraEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggkA/KCWhcqToHAw
DAYDVR0TBAUwAwEB/zAKBggqhkjOPQQDAgNHADBEAiBasbuinP+pJTU4oDCVD8zQ
1rJBDSOKIEyWu84/D6Hj6wIgVMPUoO01bPhzllAa/gW8Xk/daey09SBgN3AT9pWU
TDA=
-----END CERTIFICATE-----
-----BEGIN X509 CRL-----
MIIBqzCBlDANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDERMA8GA1UEChMI
UG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EXDTExMDIxMjE0NDQw
N1oXDTExMDQxMzE0NDQwN1owKDASAgEBFw0xMTAyMTIxNDQ0MDdaMBICAQMXDTEx
MDIxMjE0NDQwN1owDQYJKoZIhvcNAQEFBQADggEBAG64jqn7VLdvnKROsbCPR8w9
xnox9vjuM2lGWema9sTuptw9EhArVSbibXZ1IPPyrEy1QOq3NukBqUW3KzOzYV5M
BxZSa28FTQxtVChWkDUIMCK8BSxy07yieFf/3A8mbfcW3ZzN4akLxOweuFp6l2H7
9oa2jeUi1BlHCZS6JYI2pHZl8qiMRiqqMleSM2k1w7TraKLNBFM8UK72brXeZjPi
nNOzdYsQDzWo1HW7dsLWLfZKoJeyqvofVDQpC5dO56kty/do89z1OnEXfzMNeVVT
```

JCeAOzuu6kdrf+9keRoWhcIoBos/XtTV57u0pgr81bLgjj5PYivevKL/kKbyvKI=
-----END X509 CRL-----
-----BEGIN DH PARAMETERS-----
MIGHAoGBAJ419DBEOgmQTzo5qXl5fQcN9TN455wkOL7052HzxxRVMyhYmwQcgJvh
1sa18fyfR9OiVEMYglOpkqVoGLN7qd5aQNNi5W7/C+VBdHTBJcGZJyyP5B3qcz32
9mLJKudlVudV0Qxk5qUJaPZ/xupz0NyoVpviuiBOI1gNi8ovSXWzAgEC
-----END DH PARAMETERS-----

Recommended key length: 160 bits

generator:
 23:84:3c:0d:55:8c:b9:7d:a9:d5:9a:80:82:fb:50:
 89:29:71:8e:8e:a1:29:2e:df:db:01:34:41:e7:66:
 fa:60:dc:bc:34:83:45:70:e0:61:e9:a6:25:23:c2:
 77:33:a9:8a:90:94:21:ff:84:d2:7b:36:39:9b:e5:
 f0:88:2b:35:98:64:28:58:27:be:fa:bf:e3:60:cc:
 c4:61:60:59:78:a7:e1:a3:b3:a7:3e:7e:5b:a8:d7:
 b7:ba:25:0e:b1:9e:79:03:b5:83:ba:43:34:b6:c1:
 ce:45:66:72:07:64:8a:af:14:d8:ae:18:19:ba:25:
 a6:d9:36:f8:8c:

prime:
 9e:a4:a8:c4:29:fe:76:18:02:4f:76:c9:29:0e:f2:
 ba:0d:92:08:9d:d9:b3:28:41:5d:88:4e:fe:3c:ae:
 c1:d4:3e:7e:fb:d8:2c:bf:7b:63:70:99:9e:c4:ac:
 d0:1e:7c:4e:22:07:d2:b5:f9:9a:9e:52:e2:97:9d:
 c3:cb:0d:66:33:75:95:a7:96:6e:69:ec:16:bd:06:
 4a:1a:dc:b2:d4:29:23:ab:2e:8f:7f:6a:84:1d:82:
 23:6e:42:8c:1e:70:3d:21:bb:b9:b9:8f:f9:fd:9c:
 53:08:e4:e8:5a:04:ca:5f:8f:73:55:ac:e1:41:20:
 c7:43:fa:8f:99:

-----BEGIN DH PARAMETERS-----
MIIBAwJ+AJ6kqMQp/nYYAk92ySkO8roNkgid2bMoQV2ITv48rsHUPn772Cy/e2Nw
mZ7ErNAefE4iB9K1+ZqeUuKXncPLDWYzdZWnlm5p7Ba9Bkoa3LLUKSOrLo9/aoQd
giNuQowecD0hu7m5j/n9nFMI5OhaBMpfj3NVrOFBIMdD+o+ZAn0jhDwNVYy5fanV
moCC+1CJKXGOjqEpLt/bATRB52b6YNy8NINFcOBh6aYlI8J3M6mKkJQh/4TSezY5
m+XwiCs1mGQoWCe++r/jYMzEYWBZeKfho7OnPn5bqNe3uiUOsZ55A7WDukM0tsHO
RWZyB2SKrxTYrhgZuiWm2Tb4jAICAKA=
-----END
 DH PARAMETERS-----
HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 0, 0) #0
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"79349bbf7cdda5799557866621c913831146733abf8c35c8c7215b5b96c4
8e9b338c74e3e99dfedf":"":"":"":"":"c6a16ab8d420706f0f34ab7fec5adca9d8ca3a133e159ca6ac43c6f8a2be22834a4
c0a0affb10d7194f1c1a5cf7322ec1ae0964ed4bf122746e087fdb5b3e91b3493d5bb98faed49e85f130fc8a459b7"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 0, 0) #1
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"ee57fc23600fb9029a9ec6c82e7b51e43e9721e4393ef9ad841d276ca9519061d92d7ddfa6628ca3":"":"":"":"":"ee26a5c8ef08a1ca8f14154d67c88f5e7ed8219d931b9842ac0039f2145539f2142b44117a998c22f590f6c9b38b465b783ecff13a7750201f7ecf1b8ab393604c73b2389336609af3440cde43298b84"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 0, 0) #2
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"ebfdad13c8f941d279dbb4de8d7706ddfdaa279f5e4428d6f785c5b2f833b69b09b71a57cf5701d4":"":"":"":"":"66e35f9b8e05a861a0b3d01c66c416d5e8b77d4d21328c625cff9163ffc92e753015aa9d7f36ae3a961681d39f271d0b627787868cec3dedc520ecb303f96a43cec67369117af268a19f5284880cb3be"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-1, 0, 0) #3
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"4fc0ec777ec5a5f3b9ea06831a36acbb9e9add057dbb73a83367ba7c163f7b99a56ab64274ee64cd":"":"":"":"":"7910a801b68a20570ab0e593bd565021c8a543ba3942bd726021a7198f1d84c8806a6f9cc12d196e1cbfebf325d0e1971746921b4d55483fc366d2ca837c4fc9751fadea7b04c0a47d1e37649f7beb6b"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 0, 0) #4
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"85a41bafaa923240dcf613a53e28d8535474e05fb59ba1eaccb5e28b1f2493675cc4f63475a69b0d":"":"":"":"":"2735fb69bfcac5b2f7f64e747c27d9957fc6a3cd0b3eee984641b2677655606e6b0ad6c875c7bf1333ab1f9b15ab1d522968059f78eaa05a70437c6974ec8e29c8ca5a0eae5464b32e9474e4fa5d4236"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 0, 0) #5
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"b64416ea406772f955fbd7da30c67f6a42e0b9a889d55454e03a88205eaafdd584dd54a40ea5c7df":"":"":"":"":"44bc26482a49da5249e8785a4e44d91ccdc6103fd666b480350ea3a09d8a8cf9e30c103f53559cbf55e13078b7c6949e4e90e1ef79ddd234166981f715b8649834c27b17bdf0f0689ed18eb850b43e85"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-1, 0, 0) #6
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"b3d4041201f4345e0a818de136c6aa7e6b0612e1ac6b3f2f26f6ec328ac7f8966dca90e162c297ef":"":"":"":"":"d9245a4a0ab0ca97e747c0d29098979e8248e53f0ec6b91678972f3b5691e7995ad2eb99640d3e9a8364891d0ff179732d633f762d6592a4d49c4e667c699b2678929c81d9bdfc74d6575f5b727f4d65"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 0, 0) #7
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"06dbf57699df40ff67287ec11573b75b47e40e643c47f4db89bb41a3cb66446449b503b38a1e21fe":"":"":"":"":"0d06c663f9105198a34229b0e3fcffd0de9a445f4fc5d5bb58b55e43cacaf0c27c07e5a9c3734e8a8e0885dd78cd1bde0777e3330d2fb3b04203f6c2749a45cb96bafba3bf9d1875dcbc46b6af558228"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 0, 0) #8
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"cc1ca95eadbd1bdb2459f44c6653c441f225685240438aff26a3447e8f504be4c42beeeffd884455":"":"":"":"":"e8f3cbe8e1f8738b4fef6ae67662524c99cefdf7b416eafc15750054ffd7c288af1c13

ee9a61d19f7163aa21f92207b66348228b56d64438ad7eec55670860fda3da9bb0773f5647c2bd03378d795c71"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-1, 0, 0) #9
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"e68bbe5c6bb3a37207e6742ddb79c0b1640fcd3512909acd16aea846c8db
1d76ede51d5562f20639":"":"":"":"":"5cfad20546a1cc19922f0be7b7d04ba7d8335684354541b1ec8ce0adf3607446c
8742d7737a566c92fcf3b2fde205197e9aa95c739d677631e28403eafed1cf45f22fe29d3979126eaaa46a4040a4c55"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 0, 0) #10
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"ac79be87bfbab344797fa6da775516be0923da6ca517407e790d1e3cb052
983146f9a757fa910ce7":"":"":"":"":"5b4444cb58df47502374fd6bda064cf1d70d253b994f1a6e5d4e62741846472d9f
1cf14a2468aafd4ca7875b31987b8ba0de9144648a82602c19e293f2668c9519be3eb8a12f15543395348aa51697b2"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-1, 0, 0) #11
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"cddc43355e651255dedf171c9aa1334452e3e830cc4c21605e927085657e
7422b68bffab74d8f78e":"":"":"":"":"e57f32e6a8a847f033802a92e6282c967eb18f3c9837b8bbe5f5e8d9d6fbc4d571
412b873944d20bb8a354f787c3004d0b5dd5a92bdbab600f55d1ccc52275715df239a1e2a79040862680f34f5cd4f1"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 0, 0) #12
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"eb1a31c96683124985c9b412d16dd899d5da8c43273b3173417ca1a9392
265b273221bbe87831466":"":"":"":"":"59e4d915349514f4aace3d9eebfd30b58e8246c7dce23bd4c4e47bb9ac8c2696
441d5b5bb2fbb2a1b585373ec5ee55071f2ea868b2df342b5f2df48cd026ddac9114f9142db999fbcde7a0c23403fb37"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 0, 0) #13
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"6a086e671327087dde91396dd73d5400d59a4fc5b26c0558b7d5321e4f2
2584409b7e6e014e7d062":"":"":"":"":"70e17ca71ad75e40ed31629cae3fa9c23374f78e020c56e551907f2252706bd4
cd4c47d099dbc072429ae53e34ed208fdae5e6ec13e5cd9b435c1b25dcbd099132570491e7c3544cf8ff2fba553c197d"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-1, 0, 0) #14
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"8b7086efac1e3c3c87c3798471d4afd028b8bab0217d403fb61206715d21
9a93505b62cd619be51b":"":"":"":"":"0dcd502c6e884a366b50f208a1b8c59ffb85dbcd72a6e2d75aea94c9692a55a45f
a7c2900a277dcd38b79cf463ac8961fe54df47bcfe5a60555ee4ea2be76faefedae3ce65db4b3f04301cf5c43ada43"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 0, 128) #0
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"7d7052a776fd2fb3d7191f733304ee8bbe4a0ceedca8020749047e879d61
0955eed916e4060e00c9":"":"fd8bb33aab2f6cdfbc541811861d518d":"99afe347540461ddf6abeb491e0715b4":"02f7
73482dd7ae66f76e381598a64ef0":"a736343844fc92511391db0addd9064dbee24c8976aa259a9e3b6368aa6de4c9bf
3a0effcda9cb0e9dc33652ab58ecb7650ed80467f76a849fb1cfc1ed0a09f7155086064db324b1e124f3fc9e614fcb"

HMAC_DRBG NIST CAVS 14.3 PR
False (SHA-1, 0, 128) #1
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"29c62afa3c52208a3fdecb43fa613f156c9eb59ac3c2d48bbd87be99d1841654124 12314140d4027141":"":"433ddaf259d14bcf897630ccaa27338c":"141146d404f284c2d02b6a10156e3382":"edc343dbffe71ab4114ac3639d445b65":"8c730f0526694d5a9a45dbab057a1975357d65afd3eff303320bd14061f9ad38759102b6c60116f6db7a6e8e7ab94c05500b4d1e357df8e957ac8937b05fb3d080a0f90674d44de1bd6f94d295c4519d"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 0, 128) #2
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"0c0d1c0328a384e697678ac87303dd62c8780b4ac33f18674ea4dce5b190d4e381eb7a5b5e12b4f1":"":"0557bc052aa8eabab0baa42ca38fbbe9":"985865c180e0bfb7cdbed11b58b5e509":"f40452f8c5b8f4cbc1675f70bb803740":"4a1f442eae6c861b622014b079dfd47543176b82bc60826cfa02d3923ef0563f8deba8362c8d1950a70e80d67189fb4d904b855ed0ac39942aa8673e0951b4876354b849a6c1c51d0c35a3f4ed4e2f22"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 0, 128) #3
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"7cad65e5cc2888ae4e960f5d143c1425fc0785db471cc55e66451d29cf65d899a281905ff9b29e87":"":"800d583b2560d2a2300132ee2d13f19f":"42eae705c2225d212fa0554ac6ac564b":"72081e7e70200f1982c3ad9cb1d3ddbe":"953e92258be7ff61b97077252ab9835231e366dfa5b635fb889c337562a2641d3aa9e46feeb2a4ea03cb73f1f801594c3cc71d2945c11a52bb0e93419df5d0854ad5f2e36d223c119e145cad507495a7"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-1, 0, 128) #4
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"3084c8811564168bf7834d9a6c9d0ad0821b13a0b66dddc5ec2c90278236c08b6f657611a16636d7":"":"9a7665b3883bed37a48b07f98efa4b8b":"28bfe9605ba856073ee69145ccdda4e0":"c26d7c962574aa587b3eb7a8c29b2e08":"36908adee4c1e7ea4e2f266b65aa7d7b5113e4b4377adadf4406bc573e04374a7e8b9b9b36eb0384e9336a9e7b4f308b463bd7aa9476154ab13181da5c2da9675a376b9c82ace5391e378fdd0cd4ef28
"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 0, 128) #5
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"a0410a32703720abf2e28e252b5b9176cb96935082bc9ef4ca7bcab78fce7da97b0158379041bd6c":"":"b70982af7b5e337cfe989703bffc09e9":"8df8b08f648518f7526c24bb95df1e44":"6775865f451ee055ed2242076debe237":"548f66f0acd9ed887ceb7f95d1c9a0c29e2f6007b92c581e615139256bea63d0fcd7a9b950e3e89419d2142c5d8f5bbcc2ba5b0dd67689b7ade01d984e303a529165dbdd140edd69c3ec6a4ddd63e091"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-1, 0, 128) #6
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"c2e9a6e2e29f47dee0e808660c446a4faff465073a97862c2ab6787095e944c5276d29bbbbd7a777":"":"358ffeab6a24f932abd4c9577f84cb13":"37578c2d9b68d43d6c83164a4c43ce37":"02a7c9575d9527a33df9fb566373db3a":"fcd318c83563f72e5a21d4a93a84254e0c3bb6d3ded55c3d5939dbd5d1525062fd587a422012437aeb88589e669e5a5d57f7ebb16e30590f6debd0eced84f8e57d47a3d123a52361145a8fab258ed19b"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 0, 128) #7
depends_on:MBEDTLS_SHA1_C

hmac_drbg_nopr:MBEDTLS_MD_SHA1:"c93859e7fed1163b070bbefcf5ffb0a66a6f5b986116adbd959d37ea3b79a197449169bb01e0143d":"":"c62840816ae06eb725be9dd3e2954cd5":"5dc60578a6a309fae33ebf162c22fab4":"00d0fac12a9b66b7ea936411f1645d4b":"ca2eb212b29d5a38cf72409cd8cb4bc401eacbc6e59c84551cdfa12c1c8fb39c29c9d49905b25953f727ac24453ccf1c6f20a4c3fa7c33b052e4e82c7fcbab70ade865d249b6a27e0b5eddccf0567d6d"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-1, 0, 128) #8
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"237a566e4a46994fb13af5b2d4321a03fdf5cc54f461daf30949f86b7b223fc341ddbe525c533339":"":"bc252901f8f5c9357722a424b0af1bb1":"6020d93df16b10c31d8802f6bb9ddfac":"f9104117190d905a30c65c0a76148c7a":"70e0611f1cf70ba93e3cc53da83fc3d6064b293e90c117ec12cc79c5e4edf845b6a5e2c4ce75ffce5d18a75e24bf51300bae6443f04a71047a8f522edb370689ef1b2cc13769865b69dc232963d90419"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 0, 128) #9
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"80c2b6fbd576cd57c38d1d1197b9e7ad43216111a1ec8b5f31dfc1a4e05c15ed96288386d0768951":"":"1af215d9b991e4f7ddc2a89fe23388a1":"d889e43410eeb2a83cb6982f38077756":"c77e7bb93115c10a56db1245e610e8b6":"af9f8c34654f44f42914070dcf1e971884902b428c7332913ddf2e342e776e01dc2fc73cd803b3a492edb15e7cc755babc23d8a5007bb0bebd7f02bd168d055948e6a5b66a3016951697617eaad371a8"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-1, 0, 128) #10
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"d8041e31215f7c843effaec3ab722e1d271753acf2ec9ace8b5730e21c0c30f9daa98580695c4572":"":"347fc86229e2e6f6af2ead186248c2f9":"a09c1b813fd11102df392d116f127de1":"0ab6c5c7f689bda8a3a7f406bf6df33d":"e09414c8f5ff2d8d6b6523729556dc1b4bba6e4cfc7a929e4561cfd32e5484918c7f21e0b533c3e3827bb8e115cc6a2aa5def3d946001564eda8cb36fa5aa771651e4837ae60beba32e01f5d59c0be0c"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 0, 128) #11
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"b0f69a20531c5b186bf8c16b25fa1de8d6817ba362a9a00ea3aa59b018b7ce8648b7f84ab925050f":"":"2905e4b0803d221ccfba43bb4f1e3338":"0460c4ba1738dd7c662e0f4337a454c5":"b5a7870dc99f5c2ead93dae773ab55c6":"a542a3ba51f4024d3876a32fd6fdaa136c024ff36b9662ed82cf580bb1d33b531b124c0e28fd0b8ec06e50dcc11132062a55bdb961a908688ddccda12be8f1242f8a5ada53939e32d8c0381250134686"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-1, 0, 128) #12
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"188ae42fbe0f4e9e17c7b0432712aaefb1667157132f8d6240fd9d19ba9f5f56f58bd08e9842e2a1":"":"88560712277f73d457f62b3769189381":"892957bfbacc684af6d31c8befca8e4d":"a9e8986ff89479fa506780b07b09c2c9":"e77187930ac661bd1a422e29cae4c67370d9e8ab0e44ea9dd86b11b2a1c5271162513587ed02df4c91b0e04158406763e72a443a196b6a2e22af72ef2732e3916cabf518fa58ab89fea5528153818a6c"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 0, 128) #13
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"ad490819bbb9e937e0d0a749eb83465470fe146ad9f3ae0b104810bbb28773e538b466319bef5d6a":"":"e01882c8b9bc52d584274912d93367e8":"20a03700499444028da4c8fc5ba42d8f":"6574be269d5ccb5d10ad5fd6add77e2d":"5662845711b5a6c04715dcb3293f091709d87703f1a449858f074858958260ccd

833d9699fcd0bcba7956f9036808984828a3a9db2041556c77b1644a7566bd8892ed53e418cb74bca1a8d65f545c3e1"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-1, 0, 128) #14
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"aa4ea001160441917ac60f6231468f7da993e136dcce82083cc6c81b69e67ead392721ea79b63e97":"":"50f89606e793786a14ed11b3026313ce":"2445d7b670fd77bb62e0c1db75671863":"32b79488b44093ee7fdb4441bc302b70":"1b803314c8ed124bf6550bc63babf09f189e59df3d8d4103567c442b6783c32b236a107d4accd7ab3e465d29f6216349baa298ebeafd3c5cc198f0880868b8c9b67d94fd53626651200f5dfc939d4128"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 128, 0) #0
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"11c0a7e1472cec70fa8c1ca15759ac5bb1c73c22db39cd7bc6ab59ff708a5c1f598e75df060e1981":"b24e392cb1f3c18af2cb50feac733e32":"":"":"":"070e603cd48d56430a5ab461a751ec2a4a6aa6fb6ee52efe9a41e4611eafdfc957184b47bbb017e484ac34c7de56cd7813feb301b5befce573ad0a254e6cfe35b77c30be6b7cb5e7efa72813c7546ba5"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 128, 0) #1
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"e05141adb678c297eebd8136885b67345b9c0c54a0ff74d826e26c9323a3da3af6e5a5a1f351cb54":"4814ea71a8e11845716b22085cc65f2b":"":"":"":"5ef29a2e7e821d529d1928e6bab16fb80d6491a98dd53695473dadead4e5142c146f1e29b101c6b1a57d8315ce34db17040c02572c6455d902303dcfcb2ad3052166de790ce0c94af78a51864efd4b12"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-1, 128, 0) #2
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"9747f5a2a27c65b0bd9202f0743afbfd247b3b05fce7d31cd3e34742cffe1c6d55f8f98dfc57953c":"c3fc8430972dfa880e2bfa66862bffde":"":"":"":"92137ebf7518354bd65d87235a81c79e13cb53e46b47fa091cfe342f0253e5ee4634e8fe5fcb967bfcdbdfaa60614bf96826875608c0f1b55967619db6df24efedc86498cad733e29ee9d9e3d6277273"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 128, 0) #3
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"a9a8a0a7b8a58c239e083fa1cd2a8c968cfc5f074bbc31473cb71f26b82cdae4223fa32702f57ee3":"3fb4c2f37714039a1a2e6c68e4818eee":"":"":"":"1b5986ccdbac7da7fe7e792ddd445ca894b6ec08424a17fed5385ff8bd03ba782b42bc5a9676acd5be8061d535930a487902923148710ff17908fcb03db7ddc0e4b10be16c0a0365db387529a2398552"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-1, 128, 0) #4
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"99d1822bc16f2e7bbeb6556c5215489ea6039f54a175ae86aaf4cef7d80ffedc37e3c68c7de03ddd":"e80fa03bd7c8f5acdda5754ef00cdb5c":"":"":"":"2236568252a384a7e75cefba04a94381941035b28de764d5b2518a98ba4e8f1d50e8230953df40db602b8959ee8f1b8831b29516f937aaf561679bac0ffb11207030ef33b26da28af93ba552c08bff97"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 128, 0) #5

depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"305a4478bb85b0cdcb99618d8753494beee617d70aec26501eef2f751cad0b1cde509806d4064422":"c3fa490a01511e8410577021a307c31b":"":"":"":"f23ceadb881b945029b78366a173c20af93e43fd8c3be0588f811af31a7ddd653610cdfc3cd875a0f114fc1b887e4fe5042eb0dc0c36746961b1b7126950aff4c01245c215156715c7efd14c76539a0d"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 128, 0) #6
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"15c178375c839866ab31b38b900ba889325baf19b84c8fadf2f78da359af10da64c42130f79f3054":"a4d50496711dcabde8e0ff21d3da7535":"":"":"":"3f38257370353677dee9127862305158b1c5b607741d62906cebf8babee4fc6cf1dee3f821d1d750c69f3ff5683d266df0a669d291f6816d86cd222b56a351c240afbb443e886ca194994b4deddc54bb"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-1, 128, 0) #7
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"7efb63ed1e07cf853fce80468049dd5ed5e55a8b58bbdd32341f137867c451d8d4e327733de89c94":"d89028d21cee2b223d634a9927ec036b":"":"":"":"477a1612c19b1c2fee232385ccdb5b2f32c845c07fa216ee410cca20245239d3220ac48770017c4d52f99a267d53e0acdf69e8f4bd1d76d463e9bdddc16bef7faf9d9baa9b9de3d397d740d685c158a0"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 128, 0) #8
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"c7209755b92bff93a059db79883b2866b51bae337aeec9e58c87e68de33545fa20870e5e70a190f6":"34aee961eccf0b92b833f2448720bdc9":"":"":"":"285692468053547638e65dfb7c8b69aac43e16be5a4ce9898ae0d0c8f567dc27945ef6e21f36d456ca248577829b90f96a887f96e9c2a6ff2616e21c7ec93093d68f60d2cb99f2c7632f856e33ea8ff4"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-1, 128, 0) #9
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"1ceecebbc42f9ea1faf7494076f7937ba827b4666d0433ecc028ee75d4f55de2b223e92625e399ad":"b431a36c996ccdb5e936da7ebd216c20":"":"":"":"64d4bacdf185dd8f6eba35dc8f79fa2cab155113e020d1f12b32bbc4bfb9c85881692a5d8933a40d9fe8f6629f74bba8a99e8db0228a13c8d7776459f73dba8e59e9820ae72f8c425ac3044079c1ebfc"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 128, 0) #10
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"d5b264cec1c7acd78b902dc14a457d30b79acd3e06a12f57cf0c3e1b8fb1befb5abb9af1f58cc9ee":"12e4101d6d4505cd43710b05d52a9194":"":"":"":"b53d3bbf4a9561904ad9e100b2601db2660f415fc5caebbb1a628b7095e6de4a3895ac5da6f2c1e1c6655d76fa5b8f75f52de41564d79b09c9d2c76c1c486f462a7164ecd76f0dfa7b5f53c0c25b7730"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 128, 0) #11
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"f440671bcbbb1bdafb22c06482ff670374cdbd69535d07980f43cfaf10aad2453d884ce5852dbb32":"8a69144ebeca59c330c9a4e0e644a7ab":"":"":"":"a5b42447f4d02504536df9e0ca8d98642a21b64a6b84bde4b2bc186c28b0f740ebdf2d60c664d4d89a867207bb8d4c62f1745cb3c971b4b2622423a4291e1cc97f

ce7128e3ecb3ec13ce08987f59b77c"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-1, 128, 0) #12
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"bef3995f0d2b1051554cf7b3235809fcd2989cafbad081630c538a7ba0695ffd95f3abeabf2a867d":"e807cfc52494119188f86bfea878f2cd":"":"":"":"527bca6b945db8f2cda7f795763eb5767cfa1a4195a9d9ae70dd8129158138e687a056b64f00d29e11c37a9740d19fbd16429ce4dae79029018b984a22c1a2b2b988558b133651234b35f21ff42edcb2"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 128, 0) #13
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"5fc1cea988adf1f7c090b14370ce169300a008a687475c464eab4611cbf3ea5583a967ef0c0ee2e7":"7fed039d998bbfa3ad62aab86c176d6a":"":"":"":"f096f7f631882f5e5a6e708d71534c19eea20a57fc210155d49fe9b872b18cc04a73cb652a03ecfa0c6dfbc174811efd0897f4bd92c916a5c835bdfb5e126048f7c17daf00a845ff024641499047097d"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-1, 128, 0) #14
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"9c88099af48f9053abec455b7bbb015364fd593a0f40175d9d7b6301d86b259606fbca7de73ce63a":"79e501b77f967a676fe398eb7c81cdde":"":"":"":"e8d53bd119d23cc57245a8b9b2d111811dc661555e389180e367e41f8c815ab4e7aaf5a238479117402ba17ea41c1104f475e11bb97cdc414409ac516b3b28b62f284c7d4093975279d3c31320c61061"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 128, 128) #0
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"03e7b41c95818eb0b667bfa8a175a82466a1e417a9b6b92fd17e98c2e50ee0db00d25c3364451e95":"126dded5eb0bc81be37c10bcd9d5f793":"dc596d188e2343802240bc7f5cc60516":"14c8ec10f5bdde6b9e75898d7f9f03d0":"31aa842afcc1daa94098241a87d6ddfc":"4739b1bcf87404a2290829bd7a61f0b391a794c71c055c7cc513b28dcb5fdc88645bc9cb490f41fab134c6b33ce9336571762754343961de671b02a47960b4b4e23c5bfb87dcc19b260b3bcb921ae325"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-1, 128, 128) #1
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"5810043ca63ef5e573e118abd09d5e9caa873d3a2a2a1c7eb574167bab56e4d1ab5c1725421be3aa":"0ef00fe3e9126bc53dd61b8d2cb9a2a4":"4e19f01001d1f550ce0dd0bd4cd3e216":"684183426fb6d102f8e2ce55c599b740":"1a80710e25c78cafb81cc119adb0a2f9":"eb4c7059612d0ab63c0f28ceb7b8f89760c3d2b508f98441412bbe0ac133cafa7e2981ac2750272ebe503622b477c67e86930c9198fe21f7288394b2e11a5302e3db03b59780c49907ef720199ea1362"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 128, 128) #2
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"c27d1abc5afd30a3025d42bf9efeb8a6f2608470db9a90f8ec4ad2a126b799402ec8a1f210d708d1":"804004607012ed7b40ff0ad8f5ca085c":"eb2393df0be0ff471d354343c43bf2ea":"92618320cace6c075dcd69a634e76666":"da54736df5d2e0daef664e905864cc1b":"eeff317050aa3bda57bdfef2d46408b3fb2e64d34d4696254c9d8a09fa1b325bb3e3a973efe7918eb03489865f5e13e9a28a0bbb43822b9ca3b209ccaa1cd5bfa5139fe

59e16248e1f468f944a0228cd"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-1, 128, 128) #3
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"3f34680939ba128c07c5dc5aa161a8703a45440ca68c8d5c2b706e7af101ae4a669b46dfa262ada2":"e423dd11cf92c537509499eb891ef5f3":"cd32c88c56858cc5f6d39199abaf4543":"2b24bc6db1ece7a32cfe57df3f6ff74c":"3c6dc6fb353ce7e131f8d09635465d2b":"9dce0b5b3c8201c98f54501afce1595eaaa6e3e6b89abb6f6112b5bd5d1fcf549bd13e51fee87f0aab345571cfe7d7b61069660bd8cb8ea33406b6026ba28d02457e2bd3ecbe836829a4d91481fc0f75"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 128, 128) #4
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"94b31b718bc40b28cc5a67ea5e891c14e1683d0e243c4868db7a613beadf1433550003dcedbd227c":"5dd27ab3ea94ac5c04f4f8c13c767354":"fe1fbaabe7a2bdf4ffdcfac0e7e214e4":"d71d9f2a6887681bef91f5c1aaca50b8":"06cfc99087437ab7754c5d626ba07083":"4186f2a9518371d123473a4c96d23a44c89af9bafe17eb2ea702902b5a955a42b05188b8daf7ec7baee352b365f46a3b880810af5c9678df5503b5e2cf9d02897be81e409145c0cdbfb83949ef327f4f"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-1, 128, 128) #5
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"6b90e0e1496de9735239ab6ec28766669c65e1a4bc0f5c04e446388a90d86a1f060ad436666204fa":"99455a5df2b13410dcb912f37c266093":"a47f245fa6f0d928c17ed8956d1535a6":"a88cdbf82362f1a2ea78ef5bbcbec7f2":"eb8da8a49c4917d71df7facd8e9399c4":"99b09a0bf4d00539f7c1f3c28b60cd86b47a33961da7a649e810a97c1388bbd712c6eb0f7df4b68cccc01b25defbec42b67f4a341c0460e7b20ab67abb34cc2a3ce5b5d7d06a186f48d95a7607ba0510"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 128, 128) #6
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"05474cf1bfa15e12bbea7cfa9852d152ea29f8442291c64a8c9dda22ca653f755d5a5f128972d4a5":"70d00e37a88b30c450580eaed5d4d60b":"651f8ad6d3ed2bf04262dc79ecf164a3":"3e693ddf993d63cd4c9d464f2c84c8a1":"53db0c0c12363bab7b1ed57d420998ac":"590e747956e6d01eadd1c9b7b1387bfb5c20693dac84f70e2c2931459b3ca9534325d84eeef1b245d17b8cd059e05a3bf998ffb517feba0b047553633dad642e8cce5c4b7110bf57aa6416edd204f780"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-1, 128, 128) #7
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"7e9a4732f5841617395ee04ade213b80785d2e4fef267d51fe13973b675bfac30716d753cf2f6232":"0e725f5e2e3f5b9cb5ec36c4a4f99e0a":"02592ab8e4e2096733e6b300eac278ca":"2f3f8e2504bfe008aa1fee1150b47f05":"2491177e84e06c3c6b48235b29c316c4":"ca50da0839de54bd9fec1a4b1d6edba1e68b47970adc36fbf88e7757af6962d9b8ead266f8aad696f920a1bfc702d8ca43c4504cfa42d7a603a55fa524c62fe49e698f21eda7025c9b840ec1b9795066"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 128, 128) #8
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"fc16d69df6254a9b7743ca43a64e9d1f5986d771b6cb069a65484fb4311a

80479a4d00a42ce16cd6":"82fdba5fb4c04bd550eb5a8e2e4b0a31":"998b27a8e314b99b4ca06593bf9d4a17":"b9770
6d6068cbf8df35b28a2bcba3b55":"c24e22cf478a61f1adf5beece947e16a":"29573d54e80e43625024d149e6ea55cce5
728bb456e86b75175d38ad95aeb4ae5c47270ae774374ca44e2230c5d1861ff954f9fd432a5e8367abe49a88ed8eda504
b991747ea9c4cf448ba504cb7de14"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-1, 128, 128) #9
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"e917537e534f9433e40f8271a799f859524ce9bb84a53caaf9eea9984d8eb
ff701eb7c5f627074bf":"682088f3ce89ee635f5c8ec25ea8c8c8":"085a9d20a2d017c4d3e57d20cba52714":"b07122c8
eeb299295858a2fd1d3b6098":"1637261b4b3e7761b5923048a46d1eb0":"be40786139aa3966fcb85198d861f5239cb
f8886ae8e814571217dd4454c8646c4c8428558ee3d80c5297add64d6d1a991c4fdcd72cf42f82d73a89b8bd2364cd11
9821b1bf54f69acd01a7586c53925"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 128, 128) #10
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"85ed8611ac58af2d6b878ebca74256d3f2f20a7a4f174822de6ea8d0cd0bd
f18d395785f0797d371":"f2612085c5d8338c9b77b9b1eb8092af":"f414629fe7ae0a21b211e09fb66512b9":"b943191
d1882a390032339bdefd19351":"4adac9816998cb105d1c4f7cd3d53764":"dd79426f61e81d86561a98853b7e187eff7
db3e8958944cc10a74e7b12db3b08bb4436bf64694c5b8bf1857e791ae7194554aef6b48d2b33ad6854bd2e9771bbea3
e08c2c083a82cb07d7242ce22db2d"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-1, 128, 128) #11
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"6652b1c0403ef16416db88e49456119115d3901cd7dce343c7183242220
94c25d85c33857daf5b28":"a580613da8ff7b06580db9a42bc0cdbb":"923014039cd117f924900cd330607d0d":"8b42
f93d2ccdfea272f7a03bf37b831d":"28ce97668d6cc92da8ee25077cb25de9":"d31dd59237b3c8b2885838840261727a
c116bae673b554fe9c8b0c64b1573a25bc4a14c1942d80563fb4165c57e1aef5c94c1f6b1f88ec6bb2bbc10ccd8149d17
5e4965d07341aba06a9426df0d0fee3"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 128, 128) #12
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"f297186aab4f63f6fb85c4f29d659d6e48fab200424d67dd52fcacfe725ad6
5c0a47de25690c0ac5":"9414f702fd050f7edb9a648cd833f8c9":"91d5eb7962ec1051004041f5d23ffc34":"94afc7023
650c2edcd8c957e320b04f0":"b6b79df82780297261e00ef05389b693":"ebbdde904350c6d803fe258a3aa7a63622f2e
9540f03b1cf687e20ef35fc5ba6b616254710cd4515eaf69abfba0ba778b87e4ce1f9f1fef34402c6e8d23efbdeb7da53a3
db733e69527d36f24000251c"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-1, 128, 128) #13
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"90899d2da97759cc609f956f5f391a0edbb422f45afa0c7274a2ef5da636fe
c70c6d926b2670b88d":"23261c0e7226d749a0d7d0166e92dae9":"8ea2e411827c5d8b54b24da8ab41a841":"b9ee1c9
923240523e7e4745ef93581bb":"bb0f785972cf68222a5eff4c7dd3e28e":"2af35b1fba0c62aae991c12d50c86ce2cc63
3224b158b157459c41a5444072e918b4c777bfc84f8000aa238a46c5d5258057866f2484971d2708c33497191a2686f8
ee9e3657616e00dfca61e0ffb8ff"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-1, 128, 128) #14
depends_on:MBEDTLS_SHA1_C
hmac_drbg_nopr:MBEDTLS_MD_SHA1:"4e8227e8422d674cdb79e52cc30b7b84f81cc05b03339704dba3e731fc81949e679a4257c5fd68a7":"2d6e4af02acaf230bf746157ec624ba7":"deebb368a79c1788528b589056b1194b":"1dbbc7a131e98344fd748edc6fec11a0":"0266e8a066dcabaf6991c7a91e1c6e56":"e51fc833a60b099e56996a66820368f5332822c8f9dffe8459c80d2512d451e1669ecf6e562a1c295fa6981fa651fdd3d8d936c18f88d5844393a2a371aaac8f485cfe92926f1a54980500edc43a0a6c"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 0, 0) #0
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"09effa3906a5e93d05530edc71e62b39c5e4da020537176c23823da52dbdbae8307656cdaf8f861471dba14533c880505874098917e338f20ef8d8a1":"":"":"":"":"d5de8a3388b11e45085f6d9a009462947631c4e74523080ccd03a0196aa56b63a93a2939f490e9456e9fce3e9000e58190991b9aed6d145ac18f65cf2b1c17eb021acc5256eb6a7e9023f62aed87d15ea4e4b328f265cc34adbc062d54524365cc9c5073a8371f35dc2f459e1d027515"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-224, 0, 0) #1
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"29a7071e686936e60c392061f71b68500dd6f11c563732fca9dec3b2f859e06a857fd94e3ca1817872d94c2b7c2f283a0d2d12a6443e95f7e700a910":"":"":"":"":"72c0f3cb7792bfebbc1ee6f65d40d118a6a1c4e04e589c8f70273b4c7b718c9df383658572b894838a311fc0aa2aa6258758b33783e192b0c3c1d322809375dc925a05605fed8c7e8fb878fb63c84ce639fd277d9955f91602a9f4777b7c3b15404c4e761ec8d466674e32136c7b8bdb"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-224, 0,
0) #2
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"abd3dafc85b23025792bcdaf9f410829d3201c1e8ca450e217e13ec2e3b744e8c54107174a6e69ad05f643ee5cec49cd47ea88c80b96a0944154b458":"":"":"":"":"152333e16b04283dfb8c43dbb3be43b5db2ec49a399facb65cebdf7ca3ed267792ba308cdb0649b0c19cb1126b144d5766b5afeca98036a1f85cd2cfe3b8071011b69b2aec382f8562d9dd4331a554f3a3ee632cff308488b30a7416be8bbdee7e250cd12f371d069a097e9eac43031a"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-224, 0, 0) #3
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"caa286c160d22af10922ee6088c269d0c963034e5fd2a85d2fc171d0c4ba0833b630a64ab09965f132a744656631bf2dd27430c7c2d1e59cdcf43a97":"":"":"":"":"4d6132b9ce70470dd36f551584ada639e74b85fb9bd3c3e350011d99f2dc0371f874e6b9d92eba3fceafe34e574c1441d0d476c475b704755a28733e31637962cae67e849bed18d77501383cdbc27ab6f60d5d8d26634ef39e2c60fcbb04a9bdda8bcfb9b2d3aeec12a21279ed553343"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-224, 0, 0) #4
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"f79156a2321ba930e15109501ead80a3b26c1747b7a9aeb922d1a9d474df64a1fc3483f10e88a7fcdde91dc06940c58bf4d747b5a9cd8cad2c2e9870":"":"":"":"":"1b3aeaff973b2e20cee947ff283277991842a22f45cce9d22c1705daa51a56ab43aaae1b51bad7a7363edc7b548a0cec6b376b925a6e35bc7dc3b4a33a7f3b57d66b1b35256908bd2d8f0495caf2539ba4475d766c21c2c2e4acff87fefb07c662eb344d9c99ed407165f8a09a22

816a"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 0, 0) #5
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"2dfeb70fc433426e23378d048b836f899cbff52d4a92c6d7d218e3aa54c06793339a752f86f03b7fcf89bef725339f16ab1cd28ec85c20594bbdf3be":"":"":"":"":"d403dd8a6f3a914933253db9cd043421e54243a34043f5ee11a3b6a627e25d944434eac22a00172caa607ebf7de55b4c4305c2b93428d5fb4cf0a649451ec7fc5da65c4894cf4d2f3d52e90993544237e5c58745441c9cb2e047513ff81d9cf980d8b12769c21cc8c06f6d583b8be3dd"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-224, 0, 0) #6
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"2c6ba987bb61c4131138bb8acd877763c2c7e1f86289a81b6b54d1d8b399b5a5ac7171c0c9c0b5943bd7f54bf72b20307834e971bb637b351a756823":"":"":"":"":"7ff01def84626825fc22a62cfe28f5f95403bb2618eff22529b6531aaf1032100944d5f9703496d165c5756c0aac55b1812a72940aa5317fb6a2944d124e7f65766f231b6bda06100c5ad0d1b37c488e0e9f11a6d8f7e4cf7337e04d094ea9de2db1bbecf40e0cc8d1fc1cf5a01cd081"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 0, 0) #7
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"ba08acc3a00b9b40d2bad8cca4909d3bbec5471f78d0bf89a805d839b8b29fb753c9e5d3674365a7055a187a238ea1cd04f482d24d856b67eb54d71a":"":"":"":"":"9ec6ad840270051313c5825295a6f7527a8b1b9b3e7c867e5642a984b11911be60614e5737d3a0d109eea4223f0d2ee63cb19be702291a771b2e2c277f2d4559176fc5adccea52492e3d3ba7d17bad5b5f487d783639467997d7668ce2173ef777f9e31dbecb6ee716b5cedc8bc5098a"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-224, 0, 0) #8
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"95413345228eadb85b67674b9981af34bd6a4ae04866229921be928c06e6a6a6fde8d31a6a88f24d6a1114ccbe08ded9d7c50c3360bcb8908a615381":"":"":"":"":"d4dc08e36f94e88f8bfb1919c13186139591edc681affb61c421d32dfda69e507d59495bcadd39b73c4036ef440dc598e339473caba60e0770ac4729264b1dbfdaf32ca6d136ef6810a6660fa5cbac91940a28053c0fa405c7b6ca5e3f147b5e0096f36b67da9fce64247cfdaad70fc0"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 0, 0) #9
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"9b6bb9589f41e8ed6969dbf1a3b3d242dd5e133711f72549334c74190e4efb1d0452016ed4fffca9561aaf219e6793bfb6fd3dd9500bd61e6a62db66":"":"":"":"":"cee02e4fe0980afe6ccbb1b0d80041ba9841461397494f0fae5188228fbe9822e3ffc5397b7caa29950d95536e7000e1249e5bb93a593e659a49689add16d2f5e02ff251c76716dc426010c2961a176bd63c29397f6e36cd4de2f2b11e1260b9f9a00bd49b4b6617fb056b82c92c471d"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-224, 0, 0) #10
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"f276ba0da08274a082f3b8ad989a713908873b742f96bbbf8c81b4e1a7

e4857bc99aeceabe534c45105306b14860883cd56f2438a7812b43f0d911f7":"":"":"":"":"24dd3eea9a8e1f9929ebbbc2a68379caec77fb42531a97f7f3a75d16ad053799ffc25cace4f4553c271ae360eca1f5131ef87bf0390b26785880db0d92bb351e6e22409d600f6dab5cbb2278b8784e67a40be4d8ea6d994115c67b7224d721d1b3c7fc5b24e15f97eb3bbe33798d1bb8"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 0, 0) #11
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"fa5ed9189f21d7e94764bddeff23050112868cfe35220b863e8112f691c57e6d6c4a91c752c5f0b37b97d5f3e383480054877f319a568b064e6562a4":"":"":"":"":"55eb5ef1248b5a34c741f2076ea5d568da630ce4720b7e2c86a9dd535b48faece2229866a36024fd4114249be4730e554b772d557ce3f8b9d4d86d91202582213a676a076b87f941351c7606a452816db5d0f8194825d402d2fe7ebb2815532091b3830a9616918bb0e3298faf037bf6"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-224, 0, 0) #12
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"d0c5003a6168163f707b25191b51211dc1ae361df1e069d0f284f66967aca4199809dc89368164213ae17285674e5574851582372fcae8cd2733bf4a":"":"":"":"":"24910e1a9304471d053af458bc3fdef527e8796e33133f5af005106b203e8fdefb274f1c0e8ff44e92c63bef3082c6e5607a7981a6076f1a1d15368f4330c7012509d5f61b4349224a87960bce9873725145f187aa931394c449f502d12b60655a0ab2a221134a51786c3683f9ffa2b2"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 0, 0) #13
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"bf5b5d1c891f7a6f2dd3f4d486d693fbf67f49584b7f053aa96ddacd9fc0cdea0fab8209d8f4335820ce68bfa04899b63cda15242e9cd3f7acb1f103":"":"":"":"":"710c8b33ab034b50a29de657b93f3c71df4727a5219a474350c88b4e3974ffd0d3452e8c4d26f579e348f39cfe0d20045a70a866c5e16a0c22aa0d69b739f74cbe8b046bc14cf82b86498460bfb26af0771371c2750f7c59320c6f6fe1d04cfb40c048686b6c1b69dc641b8957c2c341"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-224, 0, 0) #14
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"525615164dce0dac5397b357546aad049dbe5982da2c215a233557553460f8505a3e7c8224af561190099ee21a06d62f9f00e282b32b486e8d0e338f":"":"":"":"":"3fe96c9b10c4c8e43cf3cd76ced4ad85ae576f32ea6671ef284f7c97491b72152a18a1060145e4f5e7c0c373c396cb4c8c0b6d625c1f0d2ae95b0691cb1c80a3dd5eaa21632a82aaa28e09a2bbdeff7fd8812fae46deae14bbb16da24d06878fc417b3554fb47b0ef9fe18d1b9d4f4ca"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 0, 192) #0
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"ca81953d50430bfb09537a318a1a7b90a9200077abb721e55d9ac28946fbf75d9cebc81f11cf6d4db712a3b91d479e00ba30d736a763cbfe40b91448":"":"e50aa8bec96339cf2608bb82cf038d5fd6bf93e65271cb72":"5c5eed0d98c7fc7eb30acddfee002d5b99c965949d4e2095":"a1a7cbc79bfaf4571cd8020da094118d241b3f018ec823ba":"c8b7d9c15624ae018a8612edf6444354c45c6a788272281c16526c689a3dac36679e44d89c4acd7eb58ff40a577c3d1a9f4d0175feef9ac5674c115d5e4cd17f2369e0135e33b018bdc99e4099713ace986a145ef55e868f74846feb3592d44ca3ebba6044a928e9284b5ea75063ae81"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-224, 0, 192) #1
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"b96ca1202fa959ef55a683a9021068e14c75376e15d1f0394b1c091a8b6dd6b98b6f63747dae58c29186179b4155b868f5a81ca206a5086a5759b025":"":"a35096086c1fdeb1fb60dd84fa730eccedd53e5b127eecf9":"a3269fa749e55850d4aa9e466bced0beab2edf86b926c2ae":"29f6799f7c78fdfa2d0dbdde8381aec5af249556903f6313":"c63ea73e1ddc9d55bd64a63cf73f730136ab4f6d688a9cd56b945f9875ef4ff48cdbdd8b78b898486a685d8af8cccbc2a834a9804e566ee7138c7dbf488d263fbd387041f835ea46ad27cbd66721428ed5795f6ed044cdb17c8e7e3ecbf61dd68239e8fd644ae85776050afbaa06caf7"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 0, 192) #2
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"59af1213cfcaeea29e31400ab6b30f108d4a9a77d3b370972d29032cdc612b7c360c41f16b0c9d794219300fe0551e0e66d634a4eec396c50ec9604c":"":"66ed9352bed73224d35508754aab68fcea10aac06d60e888":"198a3526a67a0ce31ad0348bbdfecede4f82d4203d1d5ca1":"03faa2f4c34577cd8b2ed53e10c68c83c1ebc8d877379178":"5e24f1a9083f13274ed1020ab6935222cca644d0920839c2b142e2780983204453d2e6c58518cb351188bc3e5e3b64015882130d745511f004cfb6b64831139e01ae5bba64b74f1a1ede7e220a6d29b1067d7c68ba3543f4dda2fc97a3dd23590c2c18b85662618462ba2c05231534b6"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 0, 192) #3
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"e6cc94c72f37999f28b5fe350bff622b433ae19111786c747d954adaecba47abacfea8cdf5eab05e2f750c0a679cfb9c2c2c071461178a054af40967":"":"3032528703dd66e42c7b6b5881483eca41e9eea503852eda":"ce8c03b0a05982ceadb516b1fe513da2403a9e6dcd7a39f0":"3f7ccb55376f23dfac1dc13be617894931f9c13d15fd3dcb":"558656cad7da2ad87a7a29ec5e612addcca96d72ac7b224cde80ce386c6efda12113fe9aa8e511714a42edab53ea0289c75d34b42f2313ac366f51f5dd3f6968bbd4c09ebf840dfd03852dedc1e3b6209d932889cb04062c644482106cf8b7a237d2937840f0c4d752d52725b5590d15"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-224, 0, 192) #4
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"cd4dcc8fb50672611f19e0cc8adcf9285f9d76e7e28bcac34e931163f8057b9f86424e5d514a13c0a25bbb49ee485501ec5e21061e006ad1569d2610":"":"24480094a44067b86ef47db38ec3e62914351196358bd9d7":"c6ac3b879adb6c150a8ee44428c333574ed9b0d6806848d8":"92bdc1514d87daaa321655d56c6302878c2bde37700163e8":"21c51a1568aafb56af1fd424f6fa146113d14d6d63e1a24e3168130ebc10dd84925bc4077c41897aa8b3c73aeb5bcf392d496dedcb6487379bfb3e12bc07fcf5c196d59fcc1fa730e55c00edaa2bca7b1e32a40ba06500ed3dd7fcab361995319979a0fa9cdc406a4d20650814e8bfac"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 0, 192) #5
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"fdca0039e8485a06e6a9afbde5b07a1bbe49e13659a2164034289639d23dcf3f9874b8fb1a1af8495b6b2129b88475cc529c96271bc1bbb5c7c2ea03":"":"841f765ed5f00be838a270730ce5926659cd7cd9d5b93ca5":"825fa13ed554973768aab55917cc880183c3ebb33a532305":"736e9de931198dd1c5f18a7da3887f685fbfa22b1d6ab638":"dd8596a62847a77da81818dbbeaf0393bd5e135069ba169f8987f01dc756689342cba61d87a79d4bce2311790069d10709c3a53df974c7d6793ae1298253f13ecdbb5680928579b73d73afdcd24a703dc9b391f303d8835ba1129c3d46237ede5e44732a74f8f23b60a3a45ce42f042a"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-224, 0, 192) #6
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"e246e3f95d89c166768aac69fc95fb49eec49aa633adb938ce1705b68987aeb0fae7f57b7e99e4f3e3e1b1db2d1fedf443bd2618e95193cefd905e1d":"":"130701f88cc1e7545980e6c6f6cc76b0336f089bb66cc347":"95533f4cc247c887d6a7cc0ca753009bf034ba95b7b1d3b2":"464fd16f011eb2986d9982879d79349a3ce4f5905bbfe832":"0d4e6b03af7a648337abec2efa585908af40e88d1f104b3e8c352aa29ac79fe8e448f36b0dfd701a1fc0f1d86dcab7e8a8ecada6ba218d9aaea1c40aa442ca51f3116ced3c9b8ba7546688ed4f3a1378f76b8a29ec763784fc82906dc0f688c5e60d59e6d5284fcd96f361bc5b285465"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 0, 192) #7
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"cb0405e58270cecb34a9951adeb694c5513c499cf310f6a99985d4fb3973463e907705740e01aed4ca221d4b03ef30e69fd8dbfb4ea919a913800a1a":"":"0b57e688472e9a05baa3920417a2e8f9a9c12555fd0abc00":"cac05f79d9837c97bb39f751792624983c397fd288dd1d95":"344d2aa2b3bad1485429b66606bf215acb0a65bf2a318f6d":"b2a13d75ad389514149763199d711092a9b0e4f1e50809355cfefc1884a94f4d4a50ac5c5da0b4e9bd7537e413bb451fdd2fa77f1f894444cb5c81e4c43978ebfd96900a2c8986c885d0faf89a2ad5c6ef922dfba1b5219b0f3c4ac2095340c3b8bf0db037171b6545741c76217b2aa5"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 0, 192) #8
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"e38ea7584fea31e48ab085c44f46b4cf68ff24b4a6b0b25867463e4a46ddc9a4de23f7272af1e9c4e0391aa9491ce7cdb5f96292e0d65cb9a9a4a3cc":"":"afe267e1491de3934054b8419b88b16731217eb4ee74c854":"bd0f3c43229a0ffc9e143e16738111e16d6a06ebf3eaa5b0":"23bd14ef8cf797cff7ff787df8ed8b87684fe7a9a33bf695":"c27a6ee5bab8f8e93783840e72894f3b024c7d3206a4a1869ce6fa8b5674bcbd24d4aab30f9866d797d850423c57684b7697913b9ef7bc0be933d0e21535bd50fea0feeb293985261fb9d4eb1ef97ab5ec6b691a08db4c8171e63745d14fb4c3a03c41f906daaa2877b7622b254f0449"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-224, 0, 192) #9
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"71dc625242dcb94e6ba2bd013beb2112cfca576774e102830503b7aeda24c2c9d862f5212975ccc019ad2ea0442595f74d1d37dbcba0719d8ea32ba1":"":"0fef9f0934bb4485bfab2431f8811d963ec7fa7953ffc213":"a6a7501c4a5a93c396ef8cc969ebd93cac1c30b4783a0617":"c58ea233f35a22fd9b01592c6026aa17922070b3604c7118":"a1452d85799b54370cff65fd6dd74b575199606cc8fa64880b26972c913c372010b4c3f4ce9b7b565a8f5305072404c7b9d70f7aef6e2709c1694eefae66ffa80f16eb4b91f8041f4487427e69daa437e183e83d3b9718ba6a23fb90365884899e0d2f0bef56b27249f65e1c00c5411a"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 0, 192) #10
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"36c1e048d16f9d6035c6b62515afb929633f356fed6a654282663e2284fd4132116d21eef66d29629bc712965d960f18cf3f7dcbf8a3ccd61b5b5fb5":"":"93bb372b7ae1035de6f13b2a36c3ae5682b9a3ea8f444383":"9715b72e4755993762e11a93857f1d50a051e70d094339a5":"2f1e73945863b237f49d6d20d0999a0203f295b9a046dca2":"ca135891b47f27c26ac891df49c80d085f90c13d236a60f1372eefd81eafc5819f4ae5aee5b32d46681be01629b078ae965f67b81a5268ef0b303d09e048f4449f5aaa11af51f80151b4697b13700930167cdcb3b6e8260eeb8bec7f6a67a2050a6ea569c825d61d4858a1cd15f70fb3"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 0, 192) #11
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"582425e13356e7a840cae9fa435b220af6a96fb53ac91e7ee22023cf6a0eef3923907883ae540be816e0631c894520b86e8c6adb8152e55cb6aed5ad":"":"227762e137f9eec6d2b3c63476b404dc5b0c68613a93034a":"fba72c01a9e51c93ac00c1232c717d32fd4d4c791556e716":"f5258bf318457769a93ef5b3ba95fa2753ad1c5c1b81a785":"c753a84ba7f41af2ab757ac1e4c9c450d2112767ff55a9af8f58edc05c2adcaef7b5bf696e5c64f71d5685593f254a87625065ee0df51ab4f7bba38faf5799c567d783fa047957f3f965571a7b4cb477566d1c434d6b2e22ae16fdf473a6c03057d934a7e25f0ea3537be97238d74bc4"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-224, 0, 192) #12
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"836f5d7521f26d884dc34af2ca56ab4a752ea18b909085a87cb6d07dba32b654390a25b68ea7ba8fb790271c712f387145052ca46cb40534355c1666":"":"99d9aec334666d7c399e453455ef6ae884c2173e12e31cf2":"d74d20dc22c55c35f0b66a464dfbe8f349616916fc726298":"407b0951404079fb3b54559c0286143d9cb18957bed7fb1d":"809f372d1af60ff972049193fe9f173684a2fc9828b60b32164c1b6738e1ba6aa12cf739287a74c6ad528a3ec00095b590b44705b4975236a0b7ea02c1213f0e830f275f53bb79efd98679c4766cad27738e6fb777e98cdd606b971fa60745289d5ef72a99e1919686a53a241fe36cf0"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 0, 192) #13
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"e555ed6c7ab344fea68d73c6432e4e6da2e67d8b33ab79e5719a2def258a852d17d93212840583fe23900949c301a29fc92095f4716018144e64583b":"":"5262cccd138256fa8424801435d118f39b9aa1db4d11ca9f":"9b55d76b743bd7fc5700fde8ffca956c0ed6091df1a22aed":"f8c99af8029110c41a6a01fd2d3d12b7103aa39cbeea90c8":"d1ec06e38af7c6e0a70b73ac62bc3556183f99a47bfea0f0c4a59e7ba4b0718df5438e369ba14be84db40d5ffe8a1a5952edfb83f61ee4d984e3d2fa67f557aacc58291cc688fa29be530e66c228e68607e25c013473b4ffbcfeda721ee35f5dfc8809528eaddad8969ce719a411216f"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-224, 0, 192) #14
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"12f2cabd3b6f640daaf27ed6cf6bd7d06e2ac372733c6971739e36afe2ba1ebf4e7e5e9f5591480e3fae752fa59bb99a1949bdeccf0c100f6afe886d":"":"7766c36e6583cc8e3c26a8058fa0923bfeb3ee22033f46c0":"63e60d1bba9aa29adc3f3b8a5db53f3b703c7ae69bcbc2f7":"f416f36717ba5f0a78125ca52ccd004b2f4f2dcdd401f595":"6196b2b4adff14a26d64f440b6c160210266d7f5b77d5e292e94b8c67bd9cc774274741e7c0c9a7ab21c31f1194ef4218ddcbbe94059042d22ef44ecfecef214a73db64505d46d5493d7475d0684fc0e431c5265c12b35310d4404b3c4db6029facbaec88b0c0ae9799e5af0aa49e842"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 192, 0) #0
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"2c50da90a1f7987d5216950ea22689584b237647d96c1239f9251942f4d13d16f418b0cf7265b91c4ad97a7acbbda065a48bc1bc5c7a9ee1523c50e3":"a74c108fe870b91a2defa971fa1efcb7a209f293d29bb5ea":"":"":"":"8853eb47c4ada94a3d58a1b517784bccc8f831d02dd5239c740fd7caa3869c5ff7bbf522a78be2d510c49c496a6657a09f0ede00daee9fd77061b0f04e7342518dc6ec1f4a7ff99dd7c783882b58f5e8bc467516c6b85985fab65c6761d4fe756ffc27fd62cfb92778391a258d3b0b0e"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 192, 0) #1
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"4606e3e19a8a53e8aba05d9d1fda1ddf15e7709aa2bae8b54efc4a14e734b45a5cbbad00a749d2bde540258de74ff8fe886d05570300af2086d0b9a2":"23ef5fbde4b270c084a745e0e299a5eba228a37074fd4f07":"":"":"":"8caf86df25de5cbc3749fee4b64fe041cf4ef2859e20704bb01abe126a90ead8cffc427c2f98aac400aab97184846125a2a66888dea9c8aa108e96e03b05bbd30e566fb90c661dc1990ebfe75f73f5b0de7be419c225bfcba3713805455dffbe5d6fcc98141743b59c2cbd70e78f5977"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-224, 192, 0) #2
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"08e2e2175fb34e4111179fc2580c05afa16d224440cc7eff24082beb16133a992fc4f4e2762634fbf68177dc3f11c4d057b71661ade56e7768ab9e6b":"0a4af33e2501ba409b132459ba97603888e727aca0a0cee0":"":"":"":"39c60b6d9f85cb69b2128bde86aca2b055e21ffd7716d789f834ecacc69a043893b09459991793571d3d8070f03382a11bd1c1bf38e86fae13a932c6dc82c540fab8c8eff478e598d3295663ab75ee8a56376c0d607fe43b74ac39479b8f694a3a13826b1b96344ec67b9eb0a5858eec"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 192, 0) #3
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"b436ebeda1119de3fb2b2e532f7ebf59fac632a4d784d904f844bb73f2cade5a88d4790c8c1d5973fc73f6b7f929303b62d30b6818a25ddf705bdb9e":"07de5589726c49dc5a764de9b41bce74675e4ca3c71769a6":"":"":"":"2099fc754ecd19a19de8afd21d2ae2ce456c32d6ce7772a98e37ed47f54001f44fad8e9b591a70d3bb28f19bca22940321ba17c33193613b7b5be1ec54efa470b70cbd6be2931193c35cc73d80c139bb4e670e1a2cb74d3bedd3610e9d0f9d154372a70b608fef824c346fb16241b301"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-224, 192, 0) #4
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"4d3e993c296c66983b9c751d2c0aa2d519f801a764ac9f1fd8d86b57eb226bdd9f69efd9ad29bf16af483e7dc170f8af65c16426c2ab7c0fa9df0175":"52ae4cfe985348408d3678d60259a78369aac02953911e74":"":"":"":"bead2cfc29315133e6f5ba2e85bd7778dcf9908081032ee634f90b0124ed9371c9009419b9e2a409fe4abd6295cad57cddcb6042986cc98f2fafdff99f7cc1185f3ba0d5f1e5f5452ee5f9df03c0e8a4f8426ca246afafe81079c2f0d165b87056e7c8528e8cccac5f49d0bb5ccfbefc"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 192, 0) #5
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"c7c4e18c56e9191ba43c967cebe48e55bf9aff4d6449c3e6a1f9846bfd7f92d535bb7386c0155cdc5aa2beec888de0d432f695ec79b1c78841ad941e":"c36a381b1b36e6ab00ea80557b5e7451ec9771101dc22580":"":"":"":"da74b23d309fc7cf7670d7feb6cb6ff4da1b763ae2e8616edeec12c71511f5a24b9c466532283f4151a902ffa5ae211d7c1efa84477b93fc393ac95522f3673f97aa9e379e48d198d5929684875150633fcf8a0918d2050551d8daa91887f3d2685737b6456d0c61c0a117413f193346"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-224, 192, 0) #6
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"78426f865483ffbcc6330db2ccd65bf8f247706cedf68d4cbcc289bacb1ef32e5caf05f28a21146a9b18e77b3a7ed0d24a0803c9af7264fe4e23d692":"e5026090f9806ff6f158c4a834588f6a39e9b4a44ef2dfa6":"":"":"":"111cd64a9950cc6f20a1b38811fce4a08929ca2654bed66c0cdebab0b81552826c06ef12ce4

63fc9c91c81a35d2ca0553905922b9a4975fa8fee2c7f9ffa9f2ed8cb2609f4b7d32a44927c7b5baa8f43dda137aba9b49a
2b0394f7f67d37b7f71a5e4f4c151db6b96e8e4dd9cd0bd84d"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 192, 0) #7
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"43ca11d53ad0198e4db5e136de8136bc461851a30ce59521f931ad0596
d13365bd8297a68dd42b7dab7f40808b3ce6c12f14d4de741ce451b6637a10":"532b05891fe406ce72421013aceb4345
81be8a3a13549dfa":"":"":"":"4c42f791dc8322d779f9a1ed9a28b0cf352601a4ef6d74e4e822ee5d9eef06e700314acb7
a47dcbb62805babdcfdd236e3022374defd44bbf747764f72fbfccae10893b54b29966aba448435987c22ace4c931d01d
c945091860cae7744365bd9b619059b8b646b229878966049cf83f"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-224, 192, 0) #8
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"ddcb3024b681e30e16e05026d8e23977497fd0b2c0ac24017de2744edc
b097d3a104d4e3c6b8adcb554746f9a43671f0692c01a8f89fa98ec3a54ac7":"bd9e41974f6627ac5bbb21ec690eece45
9e1dcedefb327f9":"":"":"":"741b2a8e82aa3ca9f3a609d05a6e2d570be463ef957f235344cdf9e0f89b3610951aa1ef0b
9406785b75e59c2de8349d435e4db82fc2a4a8b94e366f4eb13c432fcf8fac08f0c7fdbe67a44e81706b53b460f78befb8
cb6dd2a0ffd13c87df84f8a5197ed47158cee171e5323593df4e"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 192, 0) #9
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"f81c4ba8605dc14072e2bda2d2ef64e71ad856061056b8d8374fff5a6fd
9a54a814fd725bda8944037197492c52c62b97ea02df33325b35b91726839":"217137084f4519d046ec896144cf2c30
1baf911e1440852e":"":"":"":"14efd71fa13dfbd498bbe13ffa24e646d04ee0ef32c99c11004c3e9d8f748ac2f956f9899a
72c8d97ae988d06275855f77a92bc30f1b957dbcfc93fffec3852715c239c5313e765affbed257d302b6d1b74977b8012
522b69902adb86efc1ad768d99d657a5375dff720b4cad886877a"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-224, 192, 0) #10
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"8181fd2cc5f7ae2d4ed2c96b9511aeeef33e50ecf164afc4eddebaf76a96
d97bfb40377959e1edc44d24df041749ec6239ff226e40d5a5feccdbeda6":"7d6ca5ab652a37cd79367d84299f1ff2c5a3
c2331c77b98e":"":"":"":"5a2cac8110a24e1d8c5f8bff3e82857ec8cfcd469c316fa18b0f65a0d30866e49fed2a228121f
50901dbbba561732c4fe82a98f341bbc0a397fd257a5f8a4a9122c991648b1a6507c82f866d26f9b22e0ee7c9a51c4d8e
5104f0b4570043c9257bb9dd6f3730f1daf94f80baf8907acb"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 192, 0) #11
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"a0ad012a978bed2268d05086b823f5d0dc9bb98ee03980d755bce968f9
ac81db886a2a05b59df40d8346334a0276b73f528db03a118545acb7f2d70e":"1a8aca3c118f2bc0c2196df81ef22c267
d20ed7c607cdae0":"":"":"":"b9dc0eb1e4aeb482dea1b4a5e6f6ef9636366face696811db2d912e9430b303f23ac95d65
682694ef9513ac5b3e56a053b2e1a2ffbcb901c375cd122cab47d31fca5a0606daf8cc2e5e6e99b90fc8ab4fa67794caad
91985cc92b2187dd2965be0980240d9be2fb1c4bf06e60f58f547"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-224, 192, 0) #12
depends_on:MBEDTLS_SHA256_C

hmac_drbg_nopr:MBEDTLS_MD_SHA224:"f28b143468ab87794230cef4361d047236444180d0cfda58cbb9494cd1ad21be96297ff799011042013789a928f18831ffb0169126dd046c774a4fce":"ea7fc50e1eea3d84bffcbf83b240e921348b532e7b33f094":"":"":"":"5c22e92f25acaf98f55ff06e1bd80d382da754d1d33cffb6fca933583ba758200357551640c439770f77f843e9ce1e9a054f69588d76acb9cb92b7a2fa2903bc51391bd7001ccc1da67a4cce9e5dd08c2d489295c36de2c148ce27311d0789310de1cab2641e92f859b036383a8058a4"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 192, 0) #13
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"b628cb448e477cb439a2de687861a992e738db6b2b25cc6c27aadfc3a0a640b3411de49c920407303e80abd7a1d4f45c4749980fe1550bff69518210":"d5f4f8266da9b7f17ac97734201544104a5c0acb53c6bf22":"":"":"":"34a834dbb7da0b6a2e2353bd9795bef369cdde4d172b3feae7b1d9fdfb0446454cfb1adeff423d0a143c33c0e0d8e7905bd1720889e8b1121f1ef82cf15443c2f9c8999c5573e7df60b52ef395ca1d1b60e7eb721c012c344d06b336d519fa2b7b6dfbed8383456504bd0b4893bf2ba2"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-224, 192, 0) #14
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"5c7c9690a1926a4580c691c2e5327e736d5c3aec0ce8f5d32d4946bc4b607f712a8759428b010ba1b268b0de64fc5eb32d3f7fa9b8d4f20fab45c72d":"0310b2d8b5655cbb0fc2041ad15a248a7b1f2ac78845e29b":"":"":"":"6f8b6df55d9d8acf87dc2af20b7f4512f9425987495f512975de8059135e7ebb8698cb0301a8816e7299e76053cb66051c8b35bd2b00b4695cff4847f168d2d60697495cd9007ab7dd74ee7f61ee90b7827543f624b7c1412bba3d6df1242e6ffd90534ed393341429fc00bd97d9bcb7"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 192, 192) #0
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"96ae702af50c50c7c38818a5133938bd7ce51197fc78e21815b6c5a7ff9c0395d764159f707d5813e5bf47c1b8232b44a007bf7decfef499d758ed53":"e96554644097e9932585b7f4bb14d101f24c8b0376f38c05":"3f698a5f6f4fe67ef2ddf23bd5a67c1a2df4f3b19425fb85":"fe1f6a90fc0ed396bca21c0d40a1bb583eb63df78c98adac":"5942b56148f27dd5388f00caa47ffd4925e854237fe14454":"150b9260ce9aa419fe1860332ae7c9f42d9ada1649679b53f46bc9d20de3431186a54afb5df7b6269cdc05540a93fdd50a2cd3a862372d862841768df02846b057993dd6aa32f874b7220a5a1fd9cb573d720a54af5715cedfc16f0d9a467735e253b2b1a6e97421fcee1f2d670dec1a"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 192, 192) #1
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"4834717f669d9b599f0ee526129057b5a7c5680724ae0459ceb0e0d4eda21e5fe92e63fd23f08f8a0b094a85f3f377fdf1018ada0c461b5a05c334e8":"870b7857dae97cd361a005c3005013e4dd55ca76e46b62bd":"522534ba1a09cf9abf29bde66ce1dacd0e273e8954eccafb":"45f54169665f59d92211f266892009958ee515f14d09581a":"4633819c2ae83c71059ec8ae41ed2c68cadf9b2085a5b8bb":"7afd6cfafd9a7bad155b59a8bb2094f76b915b93764e92858821d5c32ff4a29493788d3dc1627ffe7980950394349eba88b9c2f6869ac5086296366b6f4ee37e8529d291c9d962e30662423faf375b7820e0b650db03e3c99791d8042da790cce1a1997ea21441dba4b936bd8b393300"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-224, 192, 192) #2
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"f5d1d27eb344b63e907d82a2e57494b25dabcae440ac88738512d9602a

c8bca243018f2495599e618dde0261e43ea38d45e7c09ccdc4bf3dd8e5c100":"12ff844e5c5bb3fd871feb37ab796002846ffaca5a741c54":"f642c19602754584afa3083f567d80fdcd1e5c29202ac3ad":"cb6dbad8ce1a5677b4825cca934336b936ccf841ff98d894":"c11fcc157c643a943e54274f1d942d998fd1ea0333e21588":"6f25ae8bf8c26d5f0b9d2a81acaf221790a09241b6e83c9e527c7784881d1f7398c2d7771174f92aab45134b4633ad96430df30b130ae34af52de90b425405959ba24a41685a04d2411e2f0e8564bf5bf3280cb6d75d0b910d06c73a625cd56646eebff14fcff81411c055921cdfb4c0"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 192, 192) #3
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"49a10569d87a790d34bcc3c8fd77d075a1cef9eff337e8929b51bdb8d6c5df3ad31045684fd1dabb1fe6f052fc9886384fe43c0a7abc7adca043d35e":"34d6ad434a436a690e7644f0dc2207131148192ceb2e91b6":"8707328fc5a1721e4d72b23c2b8ca3c30ddd95664ac478aa":"82c8d83a9f5d5639a6a1ce26d244bd30dceb1cc978627e19":"2a53b0b80b29c7d071983b65ba835e4eda66bcfe7b3d90b5":"08e24ccaae3b44b7248b2d735af985dcadb84f74d202bca726de1cd663bb5ea1bb67c669126ac97218a9ca45491df90beb387615474249bba1afd4534be7a74c61fef308f13661ddfcce40f24b410cffb1cc3cbba2c6d20a5e4c4814d44bef07bb697cfcf1e9932e43349376dc04865d"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 192, 192) #4
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"9a4232a59cc579867f8330c288a9218251030c00ebe50c9cd97d6cff6e49ad079df509644ec2ebe3ad4e515654af383da265d7b348dd4b89ddd49cbd":"b4498a32f664d4b489c2b47e67845d2d2bed5096e88f86de":"b8471ee87531817d81ee32578d27fa3a190df33561da7a2d":"2e74194aa62ef911599b37a51fa742817e3a4e6c254ec179":"afc7f13ae55e738cceb976ebdd01698de4d103db797f799b":"340c28cb7cf4c3e143dac3e133de864b1f458c76e3d47f3cbb6845f940be174b8819fc539f42005f4485fddc657f064c34873094e25a9bf7ec341a98cb97014a1d694b1694170ca5a8976e86f6e4e41232f526ec8536facd02394f492fbcc7c298ef0eddb3c5a148399ded7677366cf3"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-224, 192, 192) #5
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"b89744009793d2c118365b1d2f343d6b6c59374b41dbd805e793f27882467c5342015cf968b080a88a15fd6a7be3757b05313528525ab1e2cbd08ffd":"f3c02be0a880e194013c21b09b6703a61a7ccf7a73e8a541":"bca27f10060bb8d16d499b3f6ca05ed8462b51b0b43a1fd7":"eb6fcf75884be9112219d359013f45fcb1959ea971bd0bc8":"50a03bc3652f50cb9ed1167ea70ec1e74f896f81a8090216":"d2a529722365e7ff3e660964eeb27040a0e92a4d19bbe94592cfebad71047414676ca6ca72234f5127f313cb7f5be613b44d989fe141c9a0ec1f0b4d83c36e744cfb1c72c32a02b68c21d28832da008c57664046255ef18488ed750ec5e73b18eead939f932d2809f12939670c3c1033"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 192, 192) #6
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"6d2918c15be7871cad99dc9e06f73253ef905d9705c4e4ec38664043b04f9a150fe5953bfa7aebd926be162b7edd72fdc14ff97e67dae6257ad654f4":"489243eaac215f76a573b92f0709d116bd3c817eb95c2c39":"0a84cad7a1cd21a5afe6557d7d2875d9c62183cbbf49a123":"0c14578ac9504902cb9aa654086246d113039f926a87b325":"1aaab1e3a29e144cec825d29c3f42dc945cf2772ed30cb5b":"33438ba4edd0c38db99f2b6a50b35dd89aecb3491990ec4e60460bb32eb0186ff9fdc973b1b0df23ae65da31b8af5a37a69f81ab3e577a4c2c31e51cfcc4e844b044fb597e937524f59a0019ad5120c460329c982fc93e8e7a4b4e1de5619103b23a7a579633fc925d147d8fb856a

277"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 192, 192) #7
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"1330c4aef54ff84387e0372f7c8d273cecf0af2ceb32ef6edb6a4f1ace802f3b95fa69cf578e2cda1d6060ec2554eb3152507387f325d8e26009bd80":"89d7bf8f5754cedc2e1a249f693e29276170f62c29c5edae":"a6b58f33d57570f4df05bbfb792a00087d331e17417e09ef":"f57fc701e4f8f5cc2181b5357824f932f6e07679ec0d3cc7":"586c4e8c5769156cbb54c025fb01aad0b61aa6238c231656":"0bcb6ad4f2acefb549c46271d5a4ed41d7decc095137e2044b60273388c6c6d79cb89016abcad1d6a138621720b71fc11ef82fae04026e08926e94042694a0c008f99281e03da580fbb6543aca2b4596d39699b97f1fe65ec60a70b88770eb825b716a10ce41383f31db596079a9d54e"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-224, 192, 192) #8
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"3f0564b9ceee32c8944c8f2bc4b4d2179b38acc880bdb91eed466b881e2cc21df77bc3901ab5ce5ecf029a066784503f80d1857979b09c4563944433":"5d54fc715556c20f5b2d01d6b0992f1c596e5ad77f81da75":"35cb6d07862fbab4f50038097cb463aadf14e519c8834651":"abb21e501e85ad1edc66108e3b88380fddf810b10b883317":"3c690cdd997dfa9c5677bee976fa93cac21f5bbf382f7f53":"bae872c9d221b1531f85c15f466b7a3af3fa9c9c6b72bb8f5dad77f3d12df52d10347ba5d6504cd0a285c3be578bb67f0a9f0137463dc01cdcb847e7853c5db4cbb6a115ebff7b80db0406baccb0e3e68a4a4a95364c2da29466e160fece7b8ddb65dfab000c66cc8109380a601d5ed9"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 192, 192) #9
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"115c973d6df41ead464e22572dbe0761dcdb9aad930b2e55a5558075fb7c51c94efc5f8fe5dfe24d30175a89f1bbcf146037a07b324f572d0d4c27e4":"d3079ee3a3c9b2d69ee0fd316a6448bc7d8e3b730948c46d":"2348ee87bd5a3bb45d51a7b6a109043a9b6ee3db011dda28":"937fe1a7a790754bff99ad51782e8ef5b4928d0057b0c380":"3e89899f4aad241a9189ffa127c87c15b5e3bcfd80bc316d":"0ffc883aa19b3cbdeb39039fd3760160a93cd663b8b358e9fbb6300df164689303ee5f2489ab4ab2d522f6a33c93350eab553a2499b15f8ca198303ff45e946a06d8a40959f33a759c5381b3a59da22e68032abf3da3da6aadb410cb41f54b3146ce57f9bb5d28bc823e3e03c0294794"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 192, 192) #10
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"c28541425a7cf33e29adaa91f326f216de89976031977f104f44fcbcdcf4579337434613801fe4661642392db29f15f0924566e72b596b23ff7b18d5":"44650a29972aa8521d6fb9dffeb15c00903a283f20ea9914":"43cf4de0276483be1382f3cecc6a803551a40602584cd84b":"03eaa10612895db8f66d50a2210d73d1f563c3ca929d9f54":"8d2b20abc4e8890c772bcaa05cb7b3eb5025ac4cacb5f7ce":"aed27ff8eb54a7d2787e73ed2a51877c1250c0d4eaf10aaddb30409624289a9b7742cdebba54218c7c448b57f209182e214014cd180916a8c125ad438af2e5f5ca5b00f9cf063f0c307560ed4378382b4572b97088f8d24e0bdf0fc3489f64074f1155fbb1163b54c93098b841257c30"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-224, 192, 192) #11
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"dfa52082afb4dd137cb5209f6771f04eda25794280983ba1d8cd2f3d7f9

dee556ac26d8a5a368d29096ed643089b65e9ab17b5f58ec816570499fbff":"16ccfd20408082829aaf8a818885164581
c9a1bd09e9fc12":"abe13d12a9f0133bdebe14785dfef5f08a133a6cb5c26a92":"485dad7804de594356cf3c571d5f222
63c0b7cbd4dca1f1b":"5961f8177b6015ae0119d22e0a45a4aa1bcdc580f7e7f975":"ee48e57f1b5bd72c99c911d33539
52c2c143689c3cd9b474a46e4ada83811efc67f2557d323723526809825aa338a80e833c95297d6b16490db633ac1f16
48071c3ad4cdcea056c41b4eb157ffc83c3454b0cf001f1e01c31e48a61587381e293e6cff97270c1f157b069df3e591c2
f9"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 192, 192) #12
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"95f3a1aeacd07218a2ccee44c807f790e568e0032a42fdc7c8dc9a71f76
bd725aa909ddbdf5457f1dc4e69746426a9c56fbec603867633ee36a7fe62":"658b7326cf6adbf7208d37cd69547805bc
3f58fdd874e143":"d44350c7a668e64873ff97c31d79cb23b0f1620aed7c9d23":"dfefff80f10c3143b82de3392c395ab9
4ac8a2f4c0a30048":"a6d21a762aaaddcdbae9b9ecefbcb3149d514c94fe83eb21":"4f5e544491b72b84a0d0532d7f9ce
01ec2de6a05ab5056fc75d8f73bbcac5ffc38e20745d0e8aa1eacdefea6dcbb92475b5cf9ce0a617e5603b7b9fe34f4f4cb
04ade2db35cce1fd315140e3e4ab8472216c7cfdaf004181351f210b397c3147dcd279f6fc2ebd96050e996f77ad6ba1"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-224, 192, 192) #13
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"29a1897d6ea5de66e551f8c106f601e421ddd940812530df00f634682f
249aebdaf86938c895c11f9fcb0bd1fcdb183b4f8cf86b3429a5372caafe1d":"d655a179edaf4b8381a9f6a332ed5b754d
bf34f650d19867":"31c87be686b6f90f3d1b0ea90c541e16f3430292a5c4755f":"ed49403700cebec30d1057503be7baa
cbeb45bcdfd9a43a2":"952763380af3243c6c327f23cb74f8368919e0b6b9c25934":"fb29067bdb23c0f0153932523edf
32d0e3c18e46616e07f39a4b78091eca90349f636ffcf26b68a4cd0902431f2ada91bcc86dc223db4aa7a42e7cb57a8520
95704a27f9f07962880a50d2ce16c125be1e8d4f54a0cc5eaf63150c32408db6f39b22fc93b853caaba9e49581f13a8815
"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-224, 192, 192) #14
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA224:"387e31bcfffa51323a92d90713b438a1f4ded69707be3aa517e1e72d448
abbdf0a17989b3de7c43c621e904f52db52ad823daabff9c10b3fca93acfa":"e08fff320a493d70ea4cc85a4cc604664a0d
eec8f6c7666d":"969cafc33e99964833c4d0f88f906f5429b5daa552f53bf0":"8d6e6f05301ef5cefba752f3d0ef58a2577
5d6b69f6c15a4":"72292aaa69fbef6f010fa4d5bb63d6d7a595395d79a8c110":"77ead908484044482da529f9a6f4ca6e
6d8d49954d2e2d5c7dc455e03bebf484021673727bbc40adc8812600201b8c2de8e658191422b80d23502329c84c0ca
061b212952fdb2ecf3106dd20e6455f1f231e1dad1cfbf2fa019dfe9c162a670ae20b252ae2e5a4ca0eaae1c679a7fd3b"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 0, 0) #0
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"06032cd5eed33f39265f49ecb142c511da9aff2af71203bffaf34a9ca5bd
9c0d0e66f71edc43e42a45ad3c6fc6cdc4df01920a4e669ed3a85ae8a33b35a74ad7fb2a6bb4cf395ce00334a9c9a5a5d5
52":"":"":"":"":"76fc79fe9b50beccc991a11b5635783a83536add03c157fb30645e611c2898bb2b1bc215000209208cd
506cb28da2a51bdb03826aaf2bd2335d576d519160842e7158ad0949d1a9ec3e66ea1b1a064b005de914eac2e9d4f2d7
2a8616a80225422918250ff66a41bd2f864a6a38cc5b6499dc43f7f2bd09e1e0f8f5885935124"

HMAC_DRBG

NIST CAVS 14.3 PR False (SHA-256, 0, 0) #1
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"aadcf337788bb8ac01976640726bc51635d417777fe6939eded9ccc8a378c76a9ccc9d80c89ac55a8cfe0f99942f5a4d03a57792547e0c98ea1776e4ba80c007346296a56a270a35fd9ea2845c7e81e2":"":"":"":"":"17d09f40a43771f4a2f0db327df637dea972bfff30c98ebc8842dc7a9e3d681c61902f71bffaf5093607fbfba9674a70d048e562ee88f027f630a78522ec6f706bb44ae130e05c8d7eac668bf6980d99b4c0242946452399cb032cc6f9fd96284709bd2fa565b9eb9f2004be6c9ea9ff9128c3f93b60dc30c5fc8587a10de68c"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-256, 0, 0) #2
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"62cda441dd802c7652c00b99cac3652a64fc75388dc9adcf763530ac31df92145fdc897a0c1c482204ef07e0805c014bbd9bbf717467bf4b5db2aa344dd0d90997c8201b2265f4451270128f5ac05a1a":"":"":"":"":"7e41f9647a5e6750eb8acf13a02f23f3be77611e51992cedb6602c314531aff2a6e4c557da0777d4e85faefcb143f1a92e0dbac8de8b885ced62a124f0b10620f1409ae87e228994b830eca638ccdceedd3fcd07d024b646704f44d5d9c4c3a7b705f37104b45b9cfc2d933ae43c12f53e3e6f798c51be5f640115d45cf919a4"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 0, 0) #3
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"6bdc6ca8eef0e3533abd02580ebbc8a92f382c5b1c8e3eaa12566ecfb90389a38f8481cc7735827477e0e4acb7f4a0fa72eca6f1560720e6bd1ff0152c12eeff1f959462fd62c72b7dde96abcb7f79fb":"":"":"":"":"d5a2e2f254b5ae65590d4fd1ff5c758e425be4bacdeede7989669f0a22d34274fdfc2bf87135e30abdae2691629c2f6f425bd4e119904d4785ecd9328f15259563e5a71f915ec0c02b66655471067b01016fdf934a47b017e07c21332641400bbe5719050dba22c020b9b2d2cdb933dbc70f76fec4b1d83980fd1a13c4565836"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-256, 0, 0) #4
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"096ef37294d369face1add3eb8b425895e921626495705c5a03ee566b34158ec6e2e0825534d2989715cc85956e0148d1b4f7125f472c253837fa787d5acf0382a3b89c3f41c211d263052402dcc62c5":"":"":"":"":"4541f24f759b5f2ac2b57b51125077cc740b3859a719a9bab1196e6c0ca2bd057af9d3892386a1813fc8875d8d364f15e7fd69d1cc6659470415278164df656295ba9cfcee79f6cbe26ee136e6b45ec224ad379c6079b10a2e0cb5f7f785ef0ab7a7c3fcd9cb6506054d20e2f3ec610cbba9b045a248af56e4f6d3f0c8d96a23"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 0, 0) #5
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"a7dccdd431ae5726b83585b54eae4108f7b7a25c70187c0acbb94c96cc277aa894c8f4b8e195a47356a89a50d1389ab551733eee2e922f4055e53939e222e71fae730eb037443db2c7679708abb86a65":"":"":"":"":"99ba2691a622afecc9472418e6a8f9f1cdc1e3583c3bc7a2a650a1ab79dcbccbd656636c573179276e782569420c97438c06be898867f628b1c01eb570263d2c0f09c7aab536f6fba7df6aad19e05c236b645674667c03d1b6a04d7fc11177fe78933b309679f5bf26a4632b9a13e314c4bf4532428d3d95c689002b6dc1fbb1"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-256, 0, 0) #6
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"c286425ecf543a49bcc9196b0db1a80bc54e4948adba6f41712a350a02891fa6957a659a4ec2e0b7ad185483c220fd6108c2129813eea0776fba72788fdf2718759cc3c4207fa20a5fe23ac6e32cc28e":"":"":"":"":"8e1020a4fd84c99e0fc7e3f7ce48de5ed9ec9a5c2ccd624dbe6f30e2f688a31dc55957630357a5d48ca2a456241a28bfb16d8bb000877697a7ce24d9ad4d22b0c15117996f1f270b94f46d7a9bdfa7608fa1dd849177a9b8049

e51b6b7a2742623854a1fddb5efc447eed1ea1aed6f02b4b2754ecf71ea0509da2e54f524a7e7"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 0, 0) #7
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"02818bd7c1ec456ace55beeba99f646a6d3aa0ea78356ea726b763ff0dd2d656c482687d508c9b5c2a75f7ce390014e8cf319bfa63980e3cb997fd28771bb5614e3acb1149ba45c133ffbbab17433193":"":"":"":"":"19a231ff26c1865ce75d7a7185c30dd0b333126433d0c8cbf1be0d2b384d4eb3a8aff03540fbfa5f5496521a4e4a64071b44c78bd0b7e68fac9e5695c5c13fd3b9dbe7f7739781a4c8f0b980f1b17d99bce17ceb52b56866ae02456ffef83399c8cf7826f3c45c8a19315890919d20f40fc4e18d07e9c8ccd16c3327b5988f71"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-256, 0, 0) #8
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"77a5c86d99be7bc2502870f4025f9f7563e9174ec67c5f481f21fcf2b41cae4bed044ad72ee822506a6d0b1211502967778100749f01a4d35c3b4a958aafe296877e0acafd089f50bc7797a42a33ab71":"":"":"":"":"831a4da566f46289904893ef1cc1cd4ad19ee48f3857e2b69e936d10afbdc29822e85d02663d346ef3e09a848b1d9cc04f4c4c6e3b3b0e56a034e2334d34ca08f8097be307ba41d020bc94f8c1937fe85644eeb5592c2b5a2138f7ded9a5b44b200c8b5beb27597c790f94d660eb61e8248391edc3ae2d77656cbe8354275b13"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 0, 0) #9
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"0ea458cff8bfd1dd8b1addcba9c01317d53039e533104e32f96e7d342e6c7b9b935a4b66fc74c2a48757a99c399e64e36c5f3708e7b714c4ed139b4fa9e8c763af01773484005109a85e33653bb0ce98":"":"":"":"":"373a37af84fddec13645a9768d6a785ae5a2589d64cd9b37980dde2541499210c4f408335de1d585349064f3f53a2b4c5ec6dc2a09591f99ad9fad528ac83474164b45497bf167f81e66fa08463ffea917f6891e48f149fafc20622bb1172f34886feb45c26fd446a4a4e2891b4bc594186896141aaaeeb301b49e7c1a26fec7"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 0, 0) #10
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"bfb68be4ce1756d25bdfad5e0c2f8bec29360901cc4da51d423d1591cc57e1ba98afe4bd194c143e099680c504cceaabb97caf210e82498c3408790d41c320dd4a72007778389b44b7bc3c1c4b8c53f8":"":"":"":"":"409e0aa949fb3b38231bf8732e7959e943a338ea399026b744df15cbfeff8d71b3da023dcce059a88cf0d4b7475f628e4764c8bef13c70cfbbbb6da2a18aabcad919db09d04fc59765edb165147c88dd473a0f3c5ee19237ca955697e001ba654c5ee0bd26761b49333154426bc63286298a8be634fe0d72cfdeef0f3fc48eca"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-256, 0, 0) #11
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"4f6880a64610004463031d67d7924fa446c39138d4d41007e8df3d65691a93676b33b2c13600f4b1df6ca3d1960e8dd457b87b8c8f48312b5333d43b367730c0a5ad4725a16778fcb53fe136d136cbfd":"":"":"":"":"73d0f324ed186e2ad06bd1800e262bdbda79ba54e626761bd60f74f43e3bb62958ec1e2f1d940af163e1cadc124e7ebaba2f72e67efd746c7f6d0cad53ef03d859d93cff778a32ee5be172fe7fdbdc232ded360d704a6fa0f70bebe942e56478345492f49dc5c6fc346b88a58947ad250e688e8c626fe1efe7624620e571976e"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 0, 0) #12
depends_on:MBEDTLS_SHA256_C

hmac_drbg_nopr:MBEDTLS_MD_SHA256:"aae352e111843219cae8f70e7b8f6eb9bb53d246cbec1e4f07d42757143295b4b84485dccd1bf93210e322eafcbebcd9f9237f00d744d8fbff21b9d0043c258e8731817e6a5fb7b4bf5011680e5bc642":"":"":"":"":"cfb28b93522c7d61d8d3ce3f080e435e4c83c7e13a9dab788db8fef0407267a14fbc9324e090e24df5491fedfa81116869983938d4d4d7324a310c3af33a6f7938f602c5e4e63f1771cdaabdab0782b5affb54eb53047c109a9606739dd0065bd21eca331329865548783 54f5f9f852e674dd690163b0ff74c7a25e6bae8ce39"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-256, 0, 0) #13
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"589e79e339b7d2a1b879f0b0e1a7d1ad2474eaa8025b070f1ffa877b7124d4ff0961ed64dbd62065d96e75de6d2ff9d6e928388d3af48c2968527a4d2f9c2626fbc3f3f5a5d84e0583ab6f78e7f8b081":"":"":"":"":"fce6ced1ecf474d181ab331f79c3d2cc8a768ec2818de5b3fc7cf418322716d6a6853733561a497c0c25cb288d2c9fcfbca891bafd5a834c85f3603f402acf1a7b1ea92db847ed5c252a862ad4ab5e259715f1fc81da67f5230bf8be50ee8069758095f7d0e559e03f2c6072290e61794458437609e473eb66580cddaad19b71"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 0, 0) #14
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"714277d408ad87fde317f0a94732fce62f1352bdc90936673b4f1daa0925aa26d16582a99f23010b4248b88d86485419bd9fc7cb2fd5063b2c3c0c4f346ad2e3879371a9c805e59b9f2cd2cc2a40894f":"":"":"":"":"62ef7a431288252e0d736c1d4e36cc9ac37107dcd0d0e971a22444a4adae73a41eff0b11c8625e118dbc9226142fd0a6aa10ac9b190919bda44e7248d6c88874612abd77fb3716ea515a2d563237c446e2a282e7c3b0a3aef27d3427cc7d0a7d38714659c3401dbc91d3595159318ebca01ae7d7fd1c89f6ad6b604173b0c744"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-256, 0, 256) #0
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"05ac9fc4c62a02e3f90840da5616218c6de5743d66b8e0fbf833759c5928b53d2b89a17904922ed8f017a630448485452791126b8b52ee1fd9392a0a13e0083bed4186dc649b739607ac70ec8dcecf9b":"":"43bac13bae715092cf7eb280a2e10a962faf7233c41412f69bc74a35a584e54c":"3f2fed4b68d506ecefa21f3f5bb907beb0f17dbc30f6ffbba5e5861408c53a1e":"529030df50f410985fde068df82b935ec23d839cb4b269414c0ede6cffea5b68":"02ddff5173da2fcffa10215b030d660d61179e61ecc22609b1151a75f1cbcbb4363c3a89299b4b63aca5e581e73c860491010aa35de3337cc6c09ebec8c91a6287586f3a74d9694b462d2720ea2e11bbd02af33adefb4a16e6b370fa0effd57d607547bdcfbb7831f54de7073ad2a7da987a0016a82fa958779a168674b56524"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 0, 256) #1
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"1bea3296f24e9242b96ed00648ac6255007c91f7c1a5088b2482c28c834942bf71073136a5cc1eb5b5fa09e1790a0bedd714329f3fbea1df9d0b0b0d88dfe3774beb63d011935923d048e521b710dc6f":"":"4ef872fd211a426ea1085ab39eb220cc698fdfeabe49b8835d620ab7885de7a4":"d74d1669e89875852d9ccbf11c20fe3c13a621ebcb3f7edeea39a2b3379fdcf5":"0c8aa67ca310bd8e58c16aba35880f747266dbf624e88ec8f9ee9be5d08fdeb1":"ce95b98f13adcdf7a32aa34709d6e02f658ae498d2ab01ce920f69e7e42c4be1d005acf0ca6b17891dfafc620dd4cd3894f8492a5c846089b9b452483eb0b91f3649ec0b6f98d1aaabc2e42cd39c2b25081b85ab50cb723007a0fd83550f32c210b7c4150b5a6bb3b0c9e3c971a09d43acb48e410a77f824b957092aa8ef98bc"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 0, 256) #2
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"a7ea449b49db48601fc3a3d5d77081fab092b8d420ed1b266f704f9435

2dd726d11a159b60af8d20a0e37d27e6c74aa350916ab47e8cb5dc843f9fba80639103711f86be8e3aa94f8a64a3fe0e6e
5b35":"":"e2bb6768120555e7b9e0d573537a82f8f32f54560e1050b6abb1588fb3441e66":"a50cec9d1ecddb2c163d2
4019e81c31a2b350ccd3ad8181fd31bb8d1f64fa50e":"591dbbd48b51abced67f9c6269cf0133cd3dcbb5cfafcb6ef7585
69c555a5773":"0a464abcc8685158372d544635b953fcb1d3821c30aaa93982f9b788935f00f88115aad61d5cee003b3
d1cb50f3e961a501e2dd0fc7e1724778b184a4bdf9f64e110dda7446e5544a30bd49a400ea1a5411800e1edfeea349323
618afc5dc5782dc4b71d2da4d6a4785f8dd346feb9c8740ffd26bf644e3e4323ff24c30b9f10"

HMAC_DRBG NIST
CAVS 14.3 PR False (SHA-256, 0, 256) #3
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"14683ec508a29d7812e0f04a3e9d87897000dc07b4fbcfda58eb7cdabc
492e58b2243e744eb980b3ece25ce76383fd4618590e0ef4ee2bdae462f76d9324b3002559f74c370cfccf96a571d6955
703a7":"":"9ea3ccca1e8d791d22fcda621fc4d51b882df32d94ea8f20ee449313e6909b78":"16366a578b5ea4d0cb547
790ef5b4fd45d7cd845bc8a7c45e99419c8737debb4":"a68caa29a53f1ba857e484d095805dc319fe6963e4c4daaf355f
722eba746b92":"c4e7532ee816789c2d3da9ff9f4b37139a8515dbf8f9e1d0bf00c12addd79ebbd76236f75f2aa705a09f
7955038ebff0d566911c5ea13214e2c2eeb46d23ad86a33b60f7b9448d63eec3e1d59f48b39552857447dc5d7944667a
230e3dbfa30ca322f6eacaf7536a286706a627c5083c32de0658b9073857c30fb1d86eb8ad1b"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-256, 0, 256) #4
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"fa261fb230e2822458532ca2d5c39758750e6819a6fcebef10579ba9950
96959564e1c9fbcb12878df2bd49202cbf821bf7de29e99e7f0e1b9f96f3b1902fb4049c8c6234d20de8316ebe66d9772
5457":"":"8b7326621f6afbd44a726de48d03bcc5331f7306026c229ea9523497fbeaa88d":"33b00b31623d6160c4c67
40363a96481be14b19bc47be95641227284c366922a":"2d812c8203575790ad6b6f2ed91a49d57460de779a3e881bef
3be12e8766dc91":"5574e0b4efc17e8ce136e592beabfe32551072bddd740929e698467b40b3991f028a22c760f70348
53cc53007e3793e3c4a600d9e9d94528f8dc09aeba86146cdde2b7f71255ae0efc529b49be2205979dba6525bfe155e88
19e8e2aeeaa285704242da90b4c4535101cc47d94b0e388a1b2e63ad0cbe158b9e1bbae9cc0007c"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 0, 256) #5
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"61f1471ced56aa04c57e1b512307d4cb92497d9592d7e9e35356e99d5
85cab1b84714e960c403a4fac06b2828cc564d97bf97db3c102edc81596d4757045fe6bdc008f35792fc6290b77d889c0
9c33a8":"":"5b8bdc41f76d98cfa71ed976ea3994706375c8841adb8b6b3b6418e3132e8832":"94c8a8fdf38a6ccb8571
c89420d899adab169214bb0dfcd43a04622e289935b2":"8a4b46e0a7a55907365f82d4ab9376509bd44728cab8cbafb0
da901012ad8dcd":"933eb159a6af7455b60e40586c064f05f1970f564281b1ebc4662701ac1f299e4eb908c4afcb2e065
191281ab576f684aefedd6904bad04d96bd93c0516c62a496c3073a0cda0676a11cc08866b0cc74f62cb9d3db48673b2
c3fbeada69f922b4b795ccba22df12ef7125909381f7d681f6b9caba02fb913c5437b98c040c576"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 0, 256) #6
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"a1d5bb7d70621dee6b668b28c56d5610c2f8ced30284cc3e0e48de331a
f0506288a49e3e54c5ea54c98b95de81bcc807b4e2426e98f6eed97a6cdf690a89ee109e84c3dca16c883c26fa4ac67163
8d8d":"":"5bd1e086ed228cfd8b55c1731fea40c3a63d022599ca2da4bb23118f4821ba62":"b754b53ac226e8ebe47a3d
31496ec822de06fca2e7ef5bf1dec6c83d05368ec3":"fa7e76b2805d90b3d89fff545010d84f67aa3a2c9eb2ba232e75f4
d53267dac3":"df6b2460688fa537df3ddfe5575fca5eb8abad56cbc4e5a618a2b4a7daf6e215c3a497974c502f9d0ec35d
e3fc2ea5d4f10de9b2aee66dcc7e7ae6357983095959b817f0383e3030771bd2ed97406acf78a1a4a5f30fa0992289c920

2e69e3eb1eabe227c11409ff430f6dfca1a923a8b17bc4b87e908007f5e9759c41482b01"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-256,
0, 256) #7
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"68f21d14525d56233c7e263482d344c388a840103a77fb20ac60ce463cabdc7959fa80ae570f3e0c60ac7e2578cec3cb7584b4166530442f06e241dd904f562167e2fdae3247ab853a4a9d4884a5fa46":"":"f6a5482f139045c5389c9246d772c782c4ebf79c3a84b5cf779f458a69a52914":"9d37b1ce99f8079993ddf0bd54bab218016685b22655a678ce4300105f3a45b7":"4c97c67026ff43c2ee730e7b2ce8cce4794fd0588deb16185fa6792ddd0d46de":"e5f8874be0a8345aabf2f829a7c06bb40e60869508c2bdef071d73692c0265f6a5bf9ca6cf47d75cbd9df88b9cb236cdfce37d2fd4913f177dbd41887dae116edfbdad4fd6e4c1a51aad9f9d6afe7fcafced45a4913d742a7ec00fd6170d63a68f986d8c2357765e4d38835d3fea301afab43a50bd9edd2dec6a979732b25292"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-256, 0, 256) #8
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"7988146cbf9598d74cf88dc314af6b25c3f7de96ae9892fb0756318cea01987e280bc1ae9bfdf8a73c2df07b82a32c9c2bbc607085232e5e12ccf7c0c19a5dc80e45eb4b3d4a147fe941fa6c13333474":"":"f3f5c1bb5da59252861753c4980c23f72be1732f899fdea7183b5c024c858a12":"44d0cfc4f56ab38fa465a659151b3461b65b2462d1ad6b3463b5cf96ad9dc577":"34fb9a3cdacc834ff6241474c4f6e73ed6f5d9ea0337ab2b7468f01ad8a26e93":"4caec9e760c4d468e47613fe50de4a366ae20ba76793744a4e14433ea4de79dc188601eb86c803b094641ab2337b99d459d37decc7d27473057be45ba848868ee0fb5f1cf303d2fcd0b3e0c36f65a65f81b3fee8778a1f22302e25dfe34e6d587fa8864e621121880f7cd55f350531c4ce0530099eec2d0059706dcd657708d9"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 0, 256) #9
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"1c974c953fa2a057c9fc9409a6843f6f839aa544bca4fa11e48afd77931d4656ed7c08285464af7a5dbdc10b944a127078146ad135acb836360d36afc50653dcc36c21662da2a6f6ae05222e75f34000":"":"263c4984c238ded333c864728663538173795021571 72cfa51371d82b1efd7b5":"79b591529f9a26a0d7c8f8fd64e354b0c134ef1f757e43f9463b3dbb7a3da1ab":"7d8f7204b0b5401ddce9e88dcf5facb9a44660a9f5f1c862748e7269c29f7964":"72e2ca257b9edaf59b50e05a144f56fb517832fb9ad3489b1e664e3d5412cbf6b2883e891703b2e73aff9ab56da1009fcdef010ab4cdab996795c8f7c47fb1192bb160353997ad39d7d5fd0e2efc9103a7c3f158246afd53fe53ca6782f809698ef5f1f0d85536780a3fd6a8bafa475891c09213088bd1a3dc169257c34a517a"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 0, 256) #10
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"56216d71984a77154569122c777ce57e1d101a6025b28163a25971d39c1c5d0f5cd148ba7e54f4975ac8e3e0f9b5d06a3580f8ca974626c77259c6e37383cb8150b4d0ab0b30e377bed0dc9d1ff1a1bf":"":"15633e3a62b21594d49d3d26c4c3509f96011d4dbb9d48bbbea1b61c453f6abe":"6068eaca85c14165b101bb3e8c387c41d3f298918c7f3da2a28786ab0738a6fc":"e34f92d2b6aeeeea4ff49bfe7e4b1f462eabb853f0e86fbae0e8b3d51409ce49":"587fdb856abc19ede9078797ecb44099e07aadcd83acdcb2b090601d653f4a14c68ab2ebdda63578c5633a825bae4c0c818f89aac58d30fd7b0b5d459a0f3d86fcad78f4bb14dfff08ad81e4ea9f487cb426e91d6e80dfed436ba38fce8d6f21ca2151c92dd5c323b077d6139c66395558f0537026c4a028affa271ef4e7ea23"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-256, 0, 256) #11
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"83eb48bedc1e9294866ab8e5322ef83f6f271f8188e8fdabe5817788bd3

1570dd6ed90bc692237f132441ede857a6629a4e5e127f992bd5ca79ee56bb8a9bccf74c21814bfaf97ffd052211e802e12e4":"":"84136e403d9ed7f4515c188213abcfaca35715fa55de6d734aec63c4606a68f1":"fe9d8ef26e2d2e94b99943148392b2b33a581b4b97a8d7a0ecd41660a61dd10b":"594dad642183ce2cdc9494d6bcb358e0e7b767c5a0fa33e456971b8754a9abd5":"86715d43ba95fbbca9b7193ea977a820f4b61ba1b7e3b8d161b6c51b09dfd5040d94c04338b14d97ed25af577186b36ae7251a486c8a2d24a35e84a95c89d669d49e307b4a368b72164135ac54d020a970a180dfbed135d2c86f01270846d5301bd73db2c431a8aa10a0a3d03d146e5fafb9a2aa0b4efc80edab06ff3b532236"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 0, 256) #12
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"ba2c94203dab2e6499d8c50dca7b5c34a6b4764834f9816631aa21b9f9c3736167db133bdefb25e395085bceee5a0afcfa8984d16d35302cda35a3a355ab9242ec96fec0652d39282d4a0abf0a80df87":"":"b6fed10255a3fea6772ae1ae6d9f6cbb9bfaa34804e58a5b786f9bc60b348ccd":"445e072244edc716d3528f0e0a20ff0cd8f819c0d031736c8da122748f24d6c6":"1f856e403c4fa035bac9aa81a20e347c7d8b213aab699d69d9d6186a06ac45c1":"79f33fc36b3b47d9ac805bdbbe699909a8d0beb689a8b2723c291bd5bf7f3ce61343d4722a14e4add36312dbb0594910c8828aff1abc159915d498106f9ffb31147478d8c9ef75d1536ba5036506b313f6e85033f8f6fea2a4de817c867a59378c53c70a2f108275daedd415c05b61c4fd5d48c54be9adb9dea6c40a2ec99ee0"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 0, 256) #13
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"0db4c51492db4fe973b4bb1c52a1e873b58fc6bb37a3a4bfc252b03b994495d1a2a3900f169bba3f78a42526c700de6229d5aab356876447e3a20d81c7e3fc6975e2b984180a91493044442999e1ca3a":"":"40b34183b4e72cdff5952b317b3d45943d0fdcfa0527f3563055f7c73ae8f892":"dc94220c99ffb595c7c4d6de8de5a6bb4b38847169e24a557ef6d879ad84149d":"b2376626fd2f5218b3ed4a5609b43aa24d371cd2176ea017c2b99cf868060021":"f0bd6bc4c506d9427a09352d9c1970b146360732841a6323f4cb602c87dedfb5ff7e6964b9144933af3c5c83017ccd6a94bdca467a504564aaa7b452591a16ff6a1e7e94ddc98f9a58016cdcb8caaed6c80671ba48cc81a832d341093dda1d4e5001ec6bf66348b21e3692a13df92538ad572bb2023822072fc95f9590293ffc"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 0, 256) #14
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"593845f0adfeffa7c169f8a610147ae8a08c0072fc0c14c3977d3de0d00b55af9e0eb2507342ee01c02beadee7d077bdaefe591697eab678c52e20013aa424b95cfd217b259757fbe17335563f5b5706":"":"cbb5be0ef9bf0555ee58955c4d971fb9baa6d6070c3f7244a4eb88b48f0793bf":"6dd878394abdc0402146ba07005327c55f4d821bfebca08d04e66824e3760ab4":"ba86a691d6cbf452b1e2fd1dfb5d31ef9ea5b8be92c4988dc5f560733b371f69":"00735cbfafac5df82e5cb28fc619b01e2ba9571dc0023d26f09c37fb37d0e809066165a97e532bf86fa7d148078e865fe1a09e27a6889be1533b459cd9cd229494b5cf4d2abf28c38180278d47281f13820276ec85effb8d45284eb9eef5d179ab4880023ab2bd08ee3f766f990286bf32430c042f5521bbfd0c7ee09e2254d7"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-256, 256, 0) #0
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"fa0ee1fe39c7c390aa94159d0de97564342b591777f3e5f6a4ba2aea342ec840dd0820655cb2ffdb0da9e9310a67c9e5e0629b6d7975ddfa96a399648740e60f1f9557dc58b3d7415f9ba9d4dbb501f6":"f2e58fe60a3afc59dad37595415ffd318ccf69d67780f6fa0797dc9aa43e144c":"":"":"":"f92d4cf99a535b20222a52a68db04c5af6f5ffc7b66a473a37a256bd8d298f9b4aa4af7e8d181e02367903f93bdb744c6c2f3f3472626b40ce9bd6a70e7b8f93992a16a76fab6b5f162568e08ee6c3e804aefd952ddd3acb791c50f2ad69e9a04028a06a9c01d3a62aca2aaf6efe69ed97a016213a2dd642b4886764072d9cbe"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 256, 0) #1
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"cff72f345115376a57f4db8a5c9f64053e7379171a5a1e81e82aad3448d17d44d1e971ec795d098b3dae14ffcbeecfd945ec80f0c00cad0ff0b7616d2a930af3f5cf23cd61be7fbf7c65be0031e93e38":"6ec0c798c240f22740cad7e27b41f5e42dccaf66def3b7f341c4d827294f83c9":"":"":"":"17a7901e2550de088f472518d377cc4cc6979f4a64f4975c74344215e4807a1234eefef99f64cb8abc3fb86209f6fc7ddd03e94f83746c5abe5360cdde4f2525ccf7167e6f0befae05b38fd6089a2ab83719874ce8f670480d5f3ed9bf40538a15aaad112db1618a58b10687b68875f00f139a72bdf043f736e4a320c06efd2c"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 256, 0) #2
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"b7099b06fc7a8a74c58219729db6b0f780d7b4fa307bc3d3f9f22bfb763596a3b8772059a135a6b61da72f375411de269aec4f56ec5e96fbd96048b9a63ac8d047aedbbeea7712e241133b1a357ecfc4":"2ac1bfb24e0b8c6ac2803e89261822b7f72a0320df2b199171b79bcbdb40b719":"":"":"":"0e1f2bfef778f5e5be671ecb4971624ec784ed2732abc4fbb98a8b482fb68737df91fd15acfad2951403ac77c5ca3edffc1e03398ae6cf6ac24a91678db5c7290abc3fa001aa02d50399326f85d2b8942199a1575f6746364740a5910552c639804d7530c0d41339345a58ff0080eccf1711895192a3817a8dc3f00f28cc10cc"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-256, 256, 0) #3
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"7ba02a734c8744b15ef8b4074fe639b32e4431762ab5b7cd4d5df675ea90672b8a424f32108607c8f1f45d97f500ee12d8f02b59b6a3dd276bc69cba68efcf11ab83ead1397afd9841786bd1bb5da97a":"3ad627433f465187c48141e30c2678106091e7a680229a534b851b8d46feb957":"":"":"":"1fb91186ba4b4459d994b4b9f4ca252c7be6294d6cdb5fe56f8ff784d4b190a1c6456e0a41223bbbdf83ed8e7cfbfa765d9d8bc7ea5f4d79ea7eccb4928081a21de4cca36620d6267f55d9a352b76fc0a57375884112c31f65ff28e76d315698c29e6c4c05cb58b0a07ae66143b4abc78b9d25c78b4121e1e45bef1a6c1793e2"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 256, 0) #4
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"9a8865dfe053ae77cb6a9365b88f34eec17ea5cbfb0b1f04d1459e7fa9c4f3cb180c0a74da3ec464df11fac172d1c63275b95108eff1fabe83613e1c4de575e72a5cdc4bb9311dd006f971a052386692":"336372ec82d0d68befad83691966ef6ffc65105388eb2d6eed826c2285037c77":"":"":"":"3c683f6d4f8f5a4018d01633dfee74266aaa68ed6fc649e81b64dfdf5f75e75d5c058d66cf5fd01a4f143a6ff695517a4a43bd3adfd1fb2c28ba9a41063140bedbffdb4d21b1ace1550d59209ec61f1e2dbacb2a9116a79cb1410bf2deca5218080aacd9c68e1d6557721a8913e23f617e30f2e594f61267d5ed81464ee730b2"

HMAC_DRBG NIST CAVS
14.3 PR False (SHA-256, 256, 0) #5
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"22c1af2f2a4c885f06988567da9fc90f34f80f6dd5101c281beef497a6a1b2f83fafdecf79a4174801f133131629037bf95a0e4bd24f0e2e9e444f511b7632868ead0d5bb3846771264e03f8ab8ed074":"80327dac486111b8a8b2c8e8381fb2d713a67695c2e660b2b0d4af696cc3e1de":"":"":"":"77a7fea2f35a188f6d1bfdd49b569d8c45e2dd431d35a18c6f432c724f1e33ae92cb89a9cf91519e50705a53199f5b572dc85c1aef8f28fb52dc7986228f66954d54eda84a86962cf25cf765bd9949876349291b1aae5f88fcf4b376912d205add4f53b2770c657946c0d82

4281f441509153f48356d9d43f8a927e0693db8fc"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-256, 256, 0) #6
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"d0840e3a8d629d5b883d33e053a341b21c674e67e1999f068c497ecfaabfd6f6071de7244ecb2fdf7ab27f2d84aa7b7a1dd1a8b59856c49a388f594c5f42cc2e4a56b3ccb8a65e7066e44c12f4344d50":"90d609527fad96ffe64ab153860346f3d237c8940555ae17b47842d82d3b0943":"":"":"":"7ab28a9b2d3ae999195553e6550cced4c2daccbe7ec9dcbb0d467fabba185b727fbfd9830242cd098f4db3cf4a85e8bf8e8d5974b62b28550922b32ed5bfc1a522b6605cf93bf8d90bdec1c5b9e59c6fc37a817d437068a87254be1f7c4618ada46fbc3a2efb02e44524e21d91be7534cf05fbfd858304b706d6a91ea1cc6ad5"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 256, 0) #7
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"2e2dd56869104492767a59778652831919e1c8b970f84e824ae4116597a0ab7f01c42a7e983641de46c82fd09b4f2f767306507cd3ca7eec667e640d270cfbb033063d97520b6b7e38ff3cea0e79d12b":"bcd9e1508fcc22820a8be07180fea5045367333b569e111b011cd57dc1858765":"":"":"":"b915726c7b8c5dc3975f1a334684b973abf6a9495d930088cf5d071548e4fd29a67b55cc561ed6949ad28150a9fb4307c1fa5f783a7ea872e8d7c7e67ff0c2906081ee915737d813c25be5c30b952a36f393e6baa56ab01adc2b4776ad7b5d036a53659877c7a4e5220a897d6c0799af37beeed91173fbe9c613c3b6b9bb28e5"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-256, 256, 0) #8
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"d1aab0f16bd47a5ccd67c22e094daa3735eae21aa57f0bcd9e053d9d0d545cb8199310dfe1b01265b8c0d2b46d6c7c9ff50cabae4e060f3971096b78e550cda2837a26a693d905db2d992d589b268f44":"625b4b8f4de72ea9cb6f70556322dc2a19d6b2b32de623f557e419a084ba60fd":"":"":"":"987e1fdfe004c619cf1e9034576707eccd849400e19c87a1fef5b0179ec51c42a2f8c45d7942d0023a023c89f188b26343627039856953698863322f58619c50a7385a2dc91fc78f94b59f0131dc2b56a0d7c699d427285da1c104b0ad1739da10d8071c23993787045dc21f0070e1e9aa1658fc8e3add73dac7262e80e0aa2ee"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 256, 0) #9
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"449480eaa100aff6f48dc6286a5a81b9728b084864f78a9da98f606a00a6a41fe53c6c5ac3da9f4726389a03f97bb64073a6d64e1966ae324388dc12c14544e9dc5ae4fcb331e99d350c456ff16f9aa0":"6b8fedc084d8e28d333aef6db3702b6351f0d24e30908cccb63794282655886b":"":"":"":"a06912d362da7eb25598857f6d65344c3e23ec3deb80c6e43158845b95eaeca241c0bbbd67ac385e24693444455cc1c2c08c1134d956b8bc93b28be9c2d3322b3e09252979dfb8d39d04c94f81bebda5c73110605a237b561216bda9ee9bdee1cc0c7728bcc8304682334ca944e467a27a85313fa5395a9c790e35defd2edb12"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 256, 0) #10
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"9a6174166e97aa4981ddf580bc01c96754b9f0ba042750aabfda1cffe56e8581d7512ff6b7db7ce141b2bb01dcd0425e6888b9277e57dc57663d402eba8d03cf56a070dc868e6a128b18040002baf690":"ed75288f23275f9422444da5d3b53ccb3c4ac8acfb659a1e9b7655c2db52f879":"":"":"":"03519dfb2ff88cc2b53eecc48ae2a18ddcf91a5d69d5aefcdda8444e6df790a5240e67b2a4de75b4bb8a31f0f8aeb5e785ffb7a1341bb52fe00a05ee66fa2d44ea9956e055f9ffa6647c3bfe851ab364ade71a0d356de710ddafb7622b1da1bc53fd4d3210407289c68d8ae

b346bf15806dbe787e781b94f63da3e1f61b5ac60"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-256, 256, 0) #11
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"9c6ae1002ee1b0add0be563ce50f899da936e13efa620d08c2688c1925
14763afde7db5160c73044be73e9d4c1b22d86bcc28fd58e397f53f494ad8132df82c5d8c4c22ea0b7139bd81eeba6566
7bb69":"8fdaaeffd64e53f7b4374d902d441209964e12b65d29afec258e65db6de167ca":"":"":"":"021d938c9b4db780
c7d8134aeff1053e5b8843370b8ae9a6749fca7199d809810f1bc8dfa49426470c30c3616f903e35fbacb23420a32f1bee
567cc32300f704246ddc0217f236ef52c3ec9e2433ca66f05c25721f7661c43f22c1a125ed5db531bd0836eb435c27eefc
7424ce9d845e1d4cc4c503097b4ffca788e674a5cb53"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 256, 0) #12
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"fe96a85b69d46b540918927bb609dc57642eeaefd46bb5da2163a0bc60
294b5822195a410d24db45589448dfe979d3fd09cb870879d3f734214f6a4bd2e08c62a2a954bebe559416d8c3551aaf
e71d6a":"20f698833a4472fd7b78fb9b0c4eb68604f166a2694c4af48dac2b2376790e1e":"":"":"":"d3e96dbe29e1fcb8
ed83b19dbfb240e6f41679fbe83853aa71446617e63e5af78cf98b331d15bccb8c673c4e5d5dcec467a1fe26a6cd1696d
0c9bc49f78139d051287df7f3ae0dbb4bbf581cb8211931063c3f4612ced53f59d1b4ebb875729139f5d2a7d60642e8f2
835eed888b7e3e49c0dffd012cd746abfa3e1c5c2308c6"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-256, 256, 0) #13
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"a4fd693ff0a8af24bcec352d3196549fd0da5ee5d99ca58416ca03ce4c5
0f38e8cd67f2bf71d4366ce61396642531ff583d2be9a0d74e6a42159ae630acebf4e15271ef7f14f3de14752be0e0e822
b11":"368969c15a4849d7593be8b162113b9298a535c148ff668a9e8b147fb3af4eba":"":"":"":"e9188fc0eaec74b2608
e21e3a40be94aaf4ae08eb684de8f8bba2d5fd3b073aa5531c938c0fc628da65725c54b5c68bb91d7d326565e96685e0a
4e7b220c50e0caf1628edba5bd755b31894f8cb90afa76e88c5eb9e61b4932444c1397dee3e32241a3fb70a3929e49f6d
a02eea54812abb3d6b5cee18f03af1e0b4958430ab3"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 256, 0) #14
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"254ff5687a6dad3f1d237dc762f58d24ef2e2c084d0a48d26a3dc81e549
0cda3f2ec392acca491e03ce47b95963a49fcb8494b1c1f1752fb6f80d732a89b08115857f7cc96e7dff05ebb822706889
917":"f806b9b4a56682c61b55cb6a334caf87ffe135adfea6d0c3fc22b39898fbd078":"":"":"":"0e527e00494d55564f9
d9b28e7110f9a61ce36c883b5be2dcb055444164cdddd1a9f2731716f22d6ff476ce413c77abfc0e946871d5481345c2e
97b4bfdd12ac03df606fc56bdb99ac7b71a69b5b9160373bbec3e9dde477180af454e7acc6bc58dc0afb4281c0de4354c
1bf599054e3800c6d60d892858865b5361f50bfca9b"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 256, 256) #0
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"cdb0d9117cc6dbc9ef9dcb06a97579841d72dc18b2d46a1cb61e314012
bdf416d0c0d01d156016d0eb6b7e9c7c3c8da88ec6f7d5a8e2e88f43986f70b86e050d07c84b931bcf18e601c5a3eee30
64c82":"6f0fb9eab3f9ea7ab0a719bfa879bf0aaed683307fda0c6d73ce018b6e34faaa":"1ab4ca9014fa98a55938316de
8ba5a68c629b0741bdd058c4d70c91cda5099b3":"16e2d0721b58d839a122852abd3bf2c942a31c84d82fca74211871
880d7162ff":"53686f042a7b087d5d2eca0d2a96de131f275ed7151189f7ca52deaa78b79fb2":"dda04a2ca7b8147af15

48f5d086591ca4fd951a345ce52b3cd49d47e84aa31a183e31fbc42a1ff1d95afec7143c8008c97bc2a9c091df0a763848391f68cb4a366ad89857ac725a53b303ddea767be8dc5f605b1b95f6d24c9f06be65a973a089320b3cc42569dcfd4b92b62a993785b0301b3fc452445656fce22664827b88f"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-256, 256, 256)
#1
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"3e42348bf76c0559cce9a44704308c85d9c205b676af0ac6ba377a5da12d32449af783973c632a490f03dbb4b4852b1e45718ac567fd2660b91c8f5f1f8f186c58c6284b6968eadc9810b7beeca148a1":"2e51c7a8ac70adc37fc7e40d59a8e5bf8dfd8f7b027c77e6ec648bd0c41a78de":"63a107246a2070739aa4bed6746439d8c2ce678a54fc887c5aba29c502da7ba9":"e4576291b1cde51c5044fdc5375624cebf63333c58c7457ca7490da037a9556e":"b5a3fbd57784b15fd875e0b0c5e59ec5f089829fac51620aa998fff003534d6f":"c624d26087ffb8f39836c067ba37217f1977c47172d5dcb7d40193a1cfe20158b774558cbee8eb6f9c62d629e1bcf70a1439e46c5709ba4c94a006ba94994796e10660d6cb1e150a243f7ba5d35c8572fd96f43c08490131797e86d3ed8467b692f92f668631b1d32862c3dc43bfba686fe72fdd947db2792463e920522eb4bc"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-256, 256, 256) #2
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"b63fdd83c674699ba473faab9c358434771c5fa0348ca0faf7ebd7cf5891826b5fd204e2598d9626edab4158a8cfd95fadea5ba92f8010bb1a6a4b6fae2caa0b384165adf721253afd635d6021f764af":"2a5dfad8494306d9d4648a805c4602216a746ae3493492693a50a86d1ba05c64":"07c69d8d2b8aa1454c5c48083dd41477fda6bfcf0385638379933a60ed2e0a77":"a14e902247a3d6493d3fbc8519518b71a660e5502cf7ecfc796cfaa5b4ee4baa":"60e690e4a1eba14aec5187112a383e9991347fab7bac7cb2a40a52579a0d2718":"792b47b6ed221623bb187d63e3f039c6983d94efd5771dc9b4c40bee65924513485a6332baeda6a96f9bb431f592d73462b61d9d914a72b56fa9d87597426fb246424ebcd7abd51b2eefec8f5b839c0b3c34015342ace296b5f2218fa194b50aea1c89663460292c92c45f112ddbf6b9406f6e7ccee9c47ed2d90a27be5dd73e"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 256, 256) #3
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"dab85f98eaf0cfba013b97de4d9c264ca6fe120366cb83e8b3113c68b34e39d5d05108e1028ae67b4ea63bdc6d75eb881794885a64470744198b7d0bc24472ffe8daf3c7eb219df6ddf180e484fe0aa5":"09fed3822f6f5e5b9e575d31dc215de1607b0dfc927412618c2d8f79166dbaba":"8d74d01b582f70b92f53b43468084e1586d9b36465d333d5faaf6911e62fe40e":"ef7f6b6eb479ab05b3f9ab6dd72eac8b1e86d887f1bcae363cae386d0275a06f":"7442b2a792a6a29559bb8a515d56916ee18200580aa02e1237dd358619382d8f":"49d2cbfa0897b7d961c293c1e572fb26f28e7b956e746f6eda90454c1370a29e25303ceadc7837514dc638553b487ef9487c977c10625409178ad6506d103c487a66655d08659d92a4d5994d1c8ddb28fe60f2e49577d6e80cae1478068c98268f45e6293c9326c7f726ec89601351c0a26fd3a6549f8a41c6f58692c86594c0"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 256, 256) #4
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"0f0aa84ef12e10ae2b279e799c683441862457b9bc25581c2cd3d5b58a5b3246f74f4230c2427a52f01f39e825d250ac5222b26e79f7c3b7066d581185b1a1f6376796f3d67f59d025dd2a7b1886d258":"d02b2f53da48b923c2921e0f75bd7e6139d7030aead5aeebe46c20b9ca47a38a":"d11512457bf3b92d1b1c0923989911f58f74e136b1436f00bad440dd1d6f1209":"54d9ea7d40b7255ef3d0ab16ea9fdf29b9a281920962b5c72d97b0e371b9d816":"601cef261da8864f1e30196c827143e4c363d3fa865b808e9450b13e251d47fa":"e9847cefea3b88062ea63f92dc9e96767ce9202a6e049c98dc1dcbc6d707687bd0e98ed2cc215780c454936292e44a7c6856d664581220b8c

8ca1d413a2b81120380bfd0da5ff2bf737b60272709523745c2ced8daef6f47d1e93ef9bc141a135674cba23045e1f99a
a78f8cead12eeffff20de2008878b1f806a2652db565a"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 256, 256) #5
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"6a868ce39a3adcd189bd704348ba732936628f083de8208640dbd4273
1447d4eefdde4e22b376e5e7385e790243506990174f7f456ac06c1d789facc071701f8b60e9accebced73a634a6ad0e1a
697d4":"f7285cd5647ff0e2c71a9b54b57f04392641a4bde4a4024fa11c859fecaad713":"5463bb2241d10c970b68c3ab
c356c0fe5ef87439fc6457c5ee94be0a3fb89834":"3ab62cdbc638c1b2b50533d28f31b1758c3b8435fe24bb6d4740005
a73e54ce6":"2dbf4c9123e97177969139f5d06466c272f60d067fefadf326ccc47971115469":"8afce49dccc4ff64c65a8
3d8c0638bd8e3b7c13c52c3c59d110a8198753e96da512c7e03aeed30918706f3ad3b819e6571cfa87369c179fb9c9bb
c88110baa490032a9d41f9931434e80c40ae0051400b7498810d769fb42dddbc7aa19bdf79603172efe9c0f5d1a65372
b463a31178cbae581fa287f39c4fbf8434051b7419f"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 256, 256) #6
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"bb6b339eae26072487084ec9e4b53f2f1d4267d205042e74c77fb9ca05
91ba50c0e7bf6eb07feccbc494af4098e59d30f47fc60afbeb807236f7974d837335bc0b22288ef09ddfcb684e16b4c36a
050b":"34aeec7ed0cae83701b6477709c8654a1114212401dc91cbe7de39d71f0c06e1":"e8071ccd84ac4527e5c6e85b
0709ed867776f25ae0e04180dcb7105ecd3e3490":"fbac45b5952200ad7c4232500f2417a1c14723bdd1cc078821bc2f
e138b86597":"c4292d7dbef3ba7c18bf46bcf26776add22ab8ee206d6c722665dec6576b1bc0":"228aa2a314fcbfe6308
9ce953ac457093deaa39dd9ce2a4ece56a6028a476a98129be516d6979eff5587c032cdf4739d7ac712970f600fa781a8e
542e399661183e34e4b90c59ec5dc5cad86f91083529d41c77b8f36c5a8e28ba1a548223a02eaed8426f6fe9f349ebec1
1bc743e767482e3472ec2799c1f530ebdc6c03bc4b"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-256, 256, 256) #7
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"be658e56f80436039e2a9c0a62952dd7d70842244b5ab10f3b8a87d361
04e62933c9627455dfde91865aee93e5071147bef24dc9a5aa23003d3825f9b2b00e7dab571ea6ad86415dbd30c0bbdc
e7b972":"d3a6eb29b180b791984deb056d72c0608a2c9044237aecf100ccb03700064c5e":"047c29e4d1584fa70cb66e
2aa148a2aa29837c5eee64dcac60fdba356cdf90bb":"41c4792161b1b00d410cb79cd56bd311a714fb78dc3471c25bdd
7479f2e9a952":"cd4936d7bc3ea0e7201bcbefbc908215a97680ca6ce8672360aea600b6564308":"2c25557f6db07db0
57f56ad5b6dc0427d1a0e825c48c19a526f9a65087c6d1ead7c78363a61616c84f1022653af65173a3f9ec3275f2b0a0d
0bc750194673c0eaa6c623cd88abb0c8979baee4cd85bfce2e4a20bfebf2c3be61676563767dfe229e0b7be67ad6fcd116
dd0b460708b1b0e5c3d60f3dd8138030404d197375d75"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 256, 256) #8
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"ae537f31a28ca14500e759716bc207983bfeab60b25079fa30b77b8d41
244cb9fca9e27d8ab84cf9b9ce491ec5d8cb671eb52777be480f05115ae6370f30159a94d50ffcc64454678ab1d1ac6f16
6fa7":"8c9cb2b19aa3abe83c8fe7da96e9c11648252653a29dcd5bf0ac334ac587f032":"9cdf6f1a2bc07acd4b0f43b5f2
b892a1153e2669f237d257923636094fb40b54":"692d512722de6ba720fd23c8994ac63179b5f7e611addf9cfacd60e0
6e144a6a":"bbeea7b2bea821f339f494947c0b4bae8056119db69a3cbef21914953729cdef":"c0c4fb7080c0fbe425c1b
756fb3a090cb0d08c7027d1bb82ed3b07613e2a757f83a78d42f9d8653954b489f800a5e058ebc4f5a1747526541d844
8cb72e2232db20569dc96342c36672c4be625b363b4587f44557e58cedb4597cb57d006fda27e027818ae89e15b4c638

2b9e7a4453290ea43163b4f9cae38b1023de6a47f7b"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 256, 256) #9
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"2f8994c949e08862db0204008f55d3561f3e0362df13b9d9a70fda39938f2d331bf3e94ea858160b832fe85d301256f55ecdb1e8fe12260b9bfe12d6e6f161474fa2311e12e39b0beb0fcd92a6737b73":"b46671cf7fa142e7012ed261e1fe86714711c246c7d1c0330fa692141e86d5d1":"3ce9a29f0207d079e6dc81fb830356e555f96a23ea71424972ea9308965786d3":"db950000c0776cc0e049929ce021020adc42d29cd9b5d8f7117fbe6bde3e594f":"fc18ee6dd3dac2306774f0ac36cd789e33462d72a8c75df9057123db33e5f7bc":"8546362cc8af9b78dd6e8eb2c37db96e70708852bfd9380abedc7f324575a167bea18f632f3e19d099cfbf310773f9719eec036d2e09f393a023add8ebdc4fb87af43b2fe6c7eaa4d39f8022ce247aa45fdc84d1b92cacce6eae8252a03ec2ec5330c01f56d113fd2ec3d0240af0afcf13ddde205bb5e7c2d912dcb4aee5dcf3"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 256, 256) #10
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"0c85e31487de1d7ba4a7b998ac56dc42c6dc0eae7bf5c8aaf1e4e78875f5fb47de878f728f73f83dc2a2f550b96c8b972d5ca8af1a70cfdccd015ee3bf0665dd1941fc6a7317b9d0d06658f5744cfbd9":"9aac37bce1a6a81dc7934e23747991e3cf48c55ffe5a57781c41768a35220a01":"db881e6d0dc3b62793d7da5fe5a18e33be9b93f4a63a00a878dfbecf0d383bd2":"f743ce1b72f3de4c901369eed581c626ed3081ca707e6634fdaff46721ce0878":"cd52da3ec8a839c537dacdea8506a3eeee879de388ff5e513322d6d1bb3ff694":"a5bdd57cb8fde6298e7c5e563afcca60dd472eca484bd8c3cc17f3307be09b601744dd3ab9e8a44107c5868824575f850c0f399b280cf198006f83ede8c0b537e9be227fa140b65995ad9dfa1f2303d560c3b7f59bedd93c1282ea263924469411c2653f87fd814c74cb91c148430481d64bad0fec3cbb3dd1f39aa55c36f81b"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 256, 256) #11
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"93161b2dc08cb0fd50171141c865a841ca935cfdd2b5907d6ff8ab0348c4ceb05cb9f6e5912b90c3349a50ab881b35a1d8e9be44b5f293482548d4787762ebfb03c73c40e45385e8b98907cd66f493dd":"0dceb4a36326c4df1685df43fddeecb5d0c76f00eb44826694f27e610290f6e1":"105a8f85d6959f3e043ef508cfea21d52123f03b7aea8034c4eec761eaba1fee":"bf781f7e489d9b4b5aa5ee6d1796468af672a8d25f311edf3c4b4dbf433d703f":"c81d6bcf1e5bf37e39dda1735c6f193df115b1a854a12e7cafe060afe4589335":"4306628124d0100fade7eaaf5edf227d50771f9e5f2e1e983800eef9a39fde0b0c280e63c8728d836b5b93ea794a32c1c04cfc54bd5300e3febb5fe2e1023eded8d7cd180279a598f76823e8d5a7dffcc93a09deec5d1f80838e938fba4de9f47e94b99382ae55f116df9c3b3ddf7e50516e203645852a415796f03a86418107"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-256, 256, 256) #12
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"1ae12a5e4e9a4a5bfa79da30a9e6c62ffc639572ef1254194d129a16eb53c7165399b3481fdf24d373222267790a0fec681554ff702658122e91ba017450cfdfc8e3f4911153f7bcc428403e9c7b9d68":"8280cfdcd7a575816e0199e115da0ea77cae9d30b49c891a6c225e9037ba67e2":"226732b7a457cf0ac0ef09fd4f81296573b49a68de5e7ac3070e148c95e8e323":"45942b5e9a1a128e85e12c34596374ddc85fd7502e5633c7390fc6e6f1e5ef56":"6fc59929b41e77072886aff45f737b449b105ed7eacbd74c7cbfedf533dbeaa1":"b7547332e1509663fcfea2128f7f3a3df484cd8df034b00199157d35d61e35f1a9d481c7d2e81305616d70fc371ee459b0b2267d627e928590edcac3231898b24ef378aa9c3d381619f665379be76c7c1bd535505c563db3725f034786e35bdd90429305fd71d7bf680e8cdd6d4c348d97078f5cf5e89dee2dc410fad4f2a30f"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 256, 256) #13
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"29e20d724dfa459960df21c6ec76b1e6cabd23a9e9456d6c591d7e4529da0ef895df1f837eba47a1687aa5c4ddcf8aaf2a2a312626ca3e20034fc4f28033c7d573f66ef61ab2ea0c7bf0411a9d247264":"3713b601e164b1a51dda1ca9242ff477514648e90d311a06e10ce5aa15da5d7f":"ec68be33ac8ff3dd127e051604898c0f9a501271859376653a0516336180993d":"9935499661d699a00c622a875441b4df5204958fe95892c8ce67f7dfb2be3e4a":"256a4ba9e8f439d5487fa5eb45efcf1bc1120491724db3abe328d951f2739fc9":"73114cb3624d687d4cd49a6e769dfc7a3f8901dc41f6ad1df4ce480536fa82e52ae958d0528640d92b8bb981b755058e32c4733682e5c4c0df41f3505a1643a0dd49cfdeaf7a18adffca88256c6d2cceb838af6c92a64bc21cb7a760a0391291bfe3575e014fc156323f8eb5e86518c669dad8d29ad5fd4ef6e296f4a0764c26"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-256, 256, 256) #14
depends_on:MBEDTLS_SHA256_C
hmac_drbg_nopr:MBEDTLS_MD_SHA256:"1353f3543eb1134980e061fc4382394975dbc74f1f1ea5ecc02780a813ac5ee6cf584db2447afbe2c8fa0c15575ee391ba60219332a67b95d90ec9de6b8453d4c8af991ae9277461ff3af1b92fc985d3":"345b0cc016f2765a8c33fc24f1dcfa182cbe29d7eacbcdc9bcda988521458fc2":"6964b9b9842aec9c7ec2aad926d701f30eec76fe699265ae2a7765d716958069":"6a03c28a9365c558c33d3fdc7e5ebf0b4d32caac70df71403fd70ced09757528":"a58546c72a0b4d47c9bd6c19e7cf4ab73b2d7ba36c6c6dc08606f608795ebd29":"5b029ef68b6799868b04dc28dbea26bc2fa9fcc8c2b2795aafeed0127b7297fa19a4ef2ba60c42ff8259d5a759f92bd90fdfb27145e82d798bb3ab7fd60bfaefb7aefb116ca2a4fa8b01d96a03c47c8d987fdd33c460e560b138891278313bb619d0c3c6f9d7c5a37e88fce83e94943705c6ff68e00484e74ad4097b0c9e5f10"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 0, 0) #0
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"096349506f3a7653d54db7ec1d09e93413edd175b6ddbeb00e56752a520ac8fffc7983b918acadaa71a67e1624f1b5024260a0495fdaba58aae41df82505012d480c8e4f751fd7ebc39f9becd694b2a3":"":"":"":"":"f4c7bec0c26cf3892d214549ac6f3d82f34c6966d4295099ee56166e879a70ecae130251facda351e903d877b6c5eab5153ce87ba6c7cf8bcc61cbd14cfbe34cf1ed43678aee69cd87b60e6bcb6ff48ebd44ce9e31982d8fe20aec34fa51d625f845f61056575969bf785c2ffab4dcc754f13de63423e94bad8d5e166d96a62a602d3ee4045df162028b89cac45e6207d9097f2b3ac0ab17729251985f276f1287f5c56cc9ba1a79fbdbb291f3a945fbfdbd63cf13b82ec91f7b1085b33279e3"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-384,
0, 0) #1
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"aece2087b713992ff49d3bf404dcda18403e015632ac03735fed29102cfea6ec1b574952687c9bad0e9aedcfc1da568be632162a83c802ab94f32bbd87f6cf4af1f2703f4a02af7d60e22383a770b9ac":"":"":"":"":"c0344807d5e3ea29fef73afb2b83dfe0aae186047fab6b603d8608df49476be18bf1f0f4707198fefa18804404887ea3c598d887e938440e1fbb8ed0a1a330cff84d952cc6405b12e7bf51b0c67d5e4896006dedb44637e393a97925890fd5176252f69d43920043844a91d0840844d89b8715052cec31e257c121d3fc0ee807b84afabee59624a00703f464b0079f12884a6e888ae4959c5423604f8ae2e6b57f4428e10b680cb74cf20417380dd5378449a24ef95d9438b0fee386badee962"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-384, 0, 0) #2

depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"c39e77d579755aacd454ab7ca6528596c397f28bcd5467cc7e0fb47f398e875da83892a840381c1bc03b7a223e92904a714dff45759124fa33464a97d7f0d7fd2d1c6c21663d31fe80abdad59458c228":"":"":"":"":"10f8ec63a550c31ecdaf2fb1b373f71f18d146ea033dd65cec2ec0b73b55bb6f3fbb7136dd045e09c4073247f093493cf26b6683bc9ebc98025f75fa405fb8deecbffeb0236a33f0ed6c7600d992ce5a268c86085adadf68047178ed89d93d739351f892723d8d6e4f428946e4e6dad1d640a9c11de23ce9b793324e31dfacfd367d86855a28cc544f88b8a91506753fa061cefcb9d77bccc15a23a84dba644089ee03db8374fee91dc23af6672159b0d2db219ffd07390b69879910b5c336a5"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 0, 0) #3
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"d2e8a25249ac850fd3b01f62cd1eae3dd94d38e724f8e2644b7bb510c37f203890242b11be773beb202e9ee93899b60a00ebf08db1648c8750b14d7b784cdf0a6d4e7cdc816469cbdc3a08d6d32503b7":"":"":"":"":"019f74eeef674ef100ba4a1835bddeb925fe6fffa97113dc00d7d8c0ed486a73e831561ae44c5bd90e189fbe2bb1bfb84f3e82ec8809699ee8c2fad80b464b6b344999c364868300c1edb065ae86109dc29516f2bdfe2a046ebc8725044c382d93990f1cba185f61f71fd22fbd076d727de32a6c1d2f430bed491c9d09eb6ee669a1dc4f8048c7be199c7cbb5aa4f14d1423c8a54763869f5dee947f776ef2543ebb88d3004739089efd86b7b22327ae952747068b35d4b3d86cac1debce3e41"

HMAC_DRBG NIST
CAVS 14.3 PR False (SHA-384, 0, 0) #4
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"cffc6c44279e641856c39f14ed35440ea2f149c77459106f960caf910af21c109067c0f9445320adfc0aaf0c86120a38584747b4049588e5d93569fcecd358c51507bed59f96145bb8db6bfb4ade3a2e":"":"":"":"":"928d6d9f9128b0af64028d5d2e94414af9f8dddd353e4155f42a5d08f3e530930e01ec0dddf25d65de7f49de702791372c71fcaf5f20bdb24eb999752bfdfca28525b16308d46cefb0bc3b260490115778161db2faebbd687b940ba098e3d5be640565b81ed9d434b6861fbb4cf034ba77380562119aa3164dc53653d4e82ec84cf351c35b1b668343faf17f172eb4c0cc3999d7d24aaba58dedf11225336b5bd747825d2ae9100cf6da3276f26cec198e52edf9194162483aa4a45fa348d0cb"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-384, 0, 0) #5
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"3a1f0474c279548c086de9e12ed754c49a0322e6631f7f441c8024fea654bb6ce245c357b13ae94064d1b41c23e5e0496199e8ac9d535f8d95fcf85fdbd31eb33c20793f35075c412ba7213194a873fb":"":"":"":"":"954b58042d028abd00f7ce3d39fdb61e0cff6c40391ef8629e87101915771b8d0c7e24292751aab1219645743c6f54306866775e28b54818c759a6bf807c4982eddd4be5e22fe35a303cd503d122cc3fc5cffe50b03117457e2efc1fd91a9768964552116811b0e65856e8f8256681c722ea2652deaa2498025e84262a3fdd78bd33bc36c057e198327a33232ecd36501a0acf997d0149b4a833153b710b90c8722b232a574d22e7026a89a4d9cc3506cc9942705a162b34db9f49301a087dfe"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 0, 0) #6
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"e5f4fa500982bdf8b023788f9a5532482b29b12e8ae776111adaa617a958ce8977873caee6e82c5098ae77287bde1d8295b8aa125923dd7f8e05df78adc29898836be76df7c5aafba6493b211cbf8b94":"":"":"":"":"5b3fc1a7ea418debe79994bc0a8c86f487ed2f320c34293db950a1a026c239b8da6226d1dea509a0fe76f5a811c9391a622343324c293a0090587c10193a2961e358d1e71c269827e0d44e93d87984f47acf5b4751c8c0661

56da1c44662af4826cdfb5f7cf98b1f0200d3a0d7b99fea7f1b17dee7acfa5baee8f95ae4e0bc050bee2eeea7c09baa729e
6e02ed19476ba3f8f5a8c1660de0353df8723efcd98f5fcaa56f6eda77f2d15c76d26989aa998c4afdc53ffcde47dafba8fe
5818e8ee"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 0, 0) #7
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"b9444339a8738df6cfe95b6dc28980d02799b2ec5c8dba9ca98fa80756
21a04172b0c9e414ea33c8bc4b3beeb536161cdb9a2a516f3e87bcc9f92ebbf4ac1a900559756903b72c4c1b5f9082d8b
341f5":"":"":"":"":"09465004f009ed378f440c10fb122a265f464d373e7f1a1719c713f6bf38d28fb5447c269c127a0c1
0081533a847c0e19f4b640be0b1edf84d95025d56679e5880922f29c942e7284296a9309b4fab1b5bd9957d470db28d3
d36a3585fd37573e8e3355d03690241d6f7211d8c6b054a813ba25f9cda76202d3270bf12f66d2e5ba5a946c7d28dd22
d55d34a30a040aa9782d1e494603143d436cbb0212fa0df6d1bbf4f19818b99a68d9cb062aaee8fa05636fc60a072ec6e
5ef24566c6b96a"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-384, 0, 0) #8
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"2aa822efa22d4cd65359107c46309033984b8e9c3ecb1b77078a09ad9e
c746ef4f64b287bcc3064867b678f81ab209db3ee132a11f8c9246ce0a3d6deb3345f9b15e4cd048289991c64a21afc46
ac98e":"":"":"":"":"7b79baf0126782bebf1794fb48633dc69ba88d63504d27a206d974854d446737da4ca1fc5bbc5436
8966b583dc441b105bb30b3be19f2778ed31564acf333b7c4cb1727480aa985afd80396866e10f6da31287cce07358d6
308e56e3bbce8613bbf472aeaecb27e66305e34af593c8631508cf7d2c512df7c9b3ab04a4ede436b9d2e6919c03a525d
ceba10afbf6e8a641591d09e8a90543f1905b08537b8868337c774c20ed47df32d115a7f3306d808bb82d06bcbdc8104
2d0a16a3fc8d0b6"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 0, 0) #9
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"a32ac0aaaee05d57cb3a626fd26854ef08a3ad42a3c688ec6a9f9b67bbff
02f86df150db0de2e3612cf106d9f158fb570901e1efb12252666e7a680513cf22bc0172c4f8c0d8b2eecfa1d471c10c9e
f8":"":"":"":"":"8271bd7aaa795b58d8f741bc207332335a68feb66ac9c3bfd5dac72f20807029f555c3bcac629d228c3a
77d596d99c5d545a8dcdd0a2fb2a5eed5c3492618dab4f763ecd7c6580817c6a7acca42d81831bfc13f38ed56ed420558
77c7f31dfad35a73eb2052f6f9183dfc89b5926680dc2aa85995d42a0c073c881f1ed332794a784553493bfd842225030
e0056d76e52810236b17f6f067d1272372395ffe9c2df3145cc65ed2c6f2f121dfc6c1eb8fa6132b44ee0373c7c027af80
383d4a7f"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 0, 0) #10
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"c586e0f5999f107281dd5c7ca1ff88d4617b4fd1bb61313895dd4bede8
75c27b5b0e6c5ba15e8725eba8fa009406aa3d8b8b66f13e07c8918c0f3f55262debfbedfc641329e1fcd6442c245626cf
d206":"":"":"":"":"9d4f4f688406d8e57d96369553ee39267a9df9020d7fa78b39e1f246675b70a8080cac5aa6967e78c
55071241e20a9446a82507a215a6c5faa3a2ea3c05c12905558d98a8eef90c8abffe6cf8b874c5ef057e365fdf179438de
6a78b4dcc075b41aace875a5dd35a44f2d2b17d6ef6aa91f79354931c4d487142f7ac2120fd78caa6c7ff5298729de16c0
e8285d73a3c6a95ada99f329dc9aa0924b0059a6585853296789b7e1129432baef4bbd2240a8ef7b19046fba104a85d4
3aee0ebf021"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-384, 0, 0) #11

depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"bcac6c2160455e7db38a9c94ebd329c1ac043b6ff607a9c76a86156974d30251b4f4b14e6cf01d407cb426ad61608d1599a6b7ba9402756bea2709cf3b162cbf040d0f5f38fc4584cb9cf4e6a7bb3984":"":"":"":"":"37d76ebbab0d4c8354086a5c5edd5aa6314a4770749d468b9e5d3454f2dbc9b25432f2d5d9f4b88bea7f9835edb22f8a7b09bd604703870abee1160369d0575bdd3847ee5fa93a9fe9aaaac0d436022f94d1b96655ab00feba1f40202425e51b084e372249fbc37f49410fc9d4d16173a9bc29181b62e342a8835f818d2647c45b6ce6c5b6f29add13d57e80513f767339575671bccdccdc9d093dbd72c91ba07d81c58ab5256b6744a94f0e75482e3848de891dabf384322d1419814cfe1590"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 0, 0) #12
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"4b667d35a481779ad919956ca06e07366a974738c09a5685fa23b3fcc1a54260cd39d725a7f2661ea86a2d57cfcd2a91e08419476bdc5534df58c6c3b077d3acd27ace0472f91854c164de7f76a9b1ac":"":"":"":"":"c82e5e2fb08171c233670e9e5403b07c600be4e91ff5b57ae284c4d733139b56ece720e82d3f9ac185e37d0f44d5281224cb5f9d230dbdfcaf1756389fe752575a2764f6ae775d0a82f2eb1d901ab04b59b54b5fadb2acc9b9af3e829ef19571dc416752b1bb0935ea2f3ad69dc452285c2f08412b11794134ba3bda0a10425576e88ea7b069b74b436aca93fe9dd1dafc78da1227b13d70157f60c9bee644451f8765e4c8badddad6c779d6b42d4e8b5ba65269186b04c38db348ab5f7a4146"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 0, 0) #13
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"c0db9453f84c2aa74bf93ef21b9e7802bb8995f6fa5e634cd4064ca2a0075319a969bad1345bb5432df63412807a646d2008394d83989cb4a506990f59f8da80e6b3a1df3fb8d726639d59cbaed1562f":"":"":"":"":"120bc268ca0d3f55d5aff5b360ca4d29a4b8ec5cb624f9674ef0a67b90bb70c238b94b2bf804fe74ca18f8364ff8b1e50b2315f8aa0c3fea663e93c80544284136de1d162e9078e9a074a50b493bcc7e0c83a0047199164a2d32133db57abb05b751a357abd3ad5298773be21c534f98645e94f0935afa53729462acbe55993b7d801bd6b0cbc8eeb5a1c5f0c0d690702f8de0a1a78dcca8862538201fafbefee55cd5be62afa8e5111c89f1f68d0f1760cecc86bf6675cb09b20e097bace037"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-384, 0, 0) #14
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"31836d292cb46aad594171e76237a3422844f62fb14d0cdf63ba587e73501051c7cbb280d4b46412e10927c9523bed1beeb5163737db7f910e444e5d5221c5469655fda4ab7218e63e1451f461b4fc70":"":"":"":"":"1cf3b49f28b791e7c81706fb1a870f1af134a0fb0d2aacfcd6e446caf0a91c04dc160f080ebd5503fb7c16ad9229bf0a7bffcaad07329d5bde4576870758a4bffebb6b5c309114688db8e59a55413b4b37689df38d72bc5358291bbcc0b05af487a33934ce626efde918d0ed5f2deb75a17bd8912a31dccd783354477fa850520c3b97b56c6d2b9e4a05d49bc36e6683271f2322c9a546fca88c502187a5f4a2035bf5c527aa312f16c357c37162d722510b52ff8357490a096692572cfd8b0f"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 0, 256) #0
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"a0c341ddf73d9404177a5fde32cbe21319c318f35cc9afca9ad41a3b06e13491e843cc6afdf2bcd00ce77ff06ce3d8a54772c46baf142e569ecd9131d6185af3575bb62a41cb646bdcae8a7a9fe60cc5":"":"b83491ec1bd89f3fc84acf1aad6fbeb8ef6ab949f41adc6d0dedc53722c171fe":"b76cec3d6300ecc4a02e810296c7e70bd9b4e7121fc5e971cbb94337980fddbd":"2a25cb0ecf913749ad46b585c76097739a14ca7b59f1f3ce4f79bc8a

4afd1378":"98c01d4527fd131cc327e9632104d9eee10407cd73ab607228d37b9b72ca2c987aa794804d505d072561c
cd5016bd4189ac9e3db9187822877dd533347b5d2071818bb7683312e1e8806e9b73b021777f7f878bb7d304ec58ce9
2e5e36d3d05a7383dc77f3fe6eb84b615f3f290bf8a43c34ef5478a30a6ad616157c9d7dd046aa66b522bcef61c9d1938
2c32425d38ed3fc049e73035af1e8b97388de22c4dcba0bdc09fd36ab7eb3f67659cbd92b8d7f6d74b56fc8daf17068c6
5fb016e29f"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 0, 256) #1
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"7817fe880c0a4224eaed0da5f3962727e4b3be567021d37d3b6d4cd779
274378f1cdab91c4e7c1433dcdcd0afbe4b43c32a2b5ffc520ac3721bfd5352fed023d04439c176288521319b5e315b6e
5e85a":"":"c7708c25003e6587fc8c8116c500d37299f5d5ffcad3405349351d4fed623874":"45f88f2df43c4b9c3d829b
7cfe61904ddf658c16043271f01c5f06ad3ec7bc32":"883cfd717ad8466035e6d3f3c04813e21657ad62eeaca449785ae
b0836ac94f8":"6e0633c532099ebf0b10d4ad35d78a48b82fbce37913e655484ae40e29772a25630a7ab37f1d0ecdce2
7773a2ce88521b171432c07c02269df1822d2b6cde0d9f768375d9c60e688f497fb7ae262cdd5f7e8b84b84411d619c3
6529b41576ac456a240ed94d750fa722db874098ef7200c74c3234a3e5f21fcbc2cb5d50c4297d1e70901b8936964ccd
242098002f4c8ed7dbf49de8c2a924c737f248d46ac1469f676377ca52cba12f28d9b534504d6e8423b5404b7e14de95
4b4225bb53551"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 0, 256) #2
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"f2bb6edec000982bfdb301d1d88a23ce840e496a4f595a662e41275712
64f1d7e9e283c567f11e7e266459fa781c6fd95339015836ebd69aa42857010f44e8a72b81f501c96931fb491dc1192f6f
6a27":"":"ecd5ea33146cb74a707eedb8df881eddb1797cbb7b16c16f8d741d23795774fc":"d410d6e2e848f2241ee45c
9870064ac0217d97f59a8e80f6b5107ff0e4240bd0":"8a8c58fde3b8c9711757cb17e46587d0c5187f758d64478e9968
604af0367136":"990b1f68152b3607f3011f8d04ea33a3e8fc479c8a6eaeb589133569048fe1284ab44d51bdcf4f0cd4c
8d64f4c6337cdbe5f4f497ea90ee4204845bebca2ffde7831cf49892829322644c4e20a45a9885ff619bdf5e79ee53c26f4
7072e20a46d2b108d180d6ba5859a696f472bfaa80b2fcc7eda374a3f91ac0b06c9f13afac1af244a389cab4489d0ee04a
0598f9c5168f39b40e7127dad9f20d69ede6cae7683b25ded1cf9d903541fb4b0a804d7c163ab068d22949f28a8f4e853
e691e51"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 0, 256) #3
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"6968f5b87019b4cdafcc9f3a89321f25ef5d8d70fd0781c9e3bb01b3ada
18c8b61d9142b639aa75f5f9d798ca538475d09b121048e8a0cc4b2286efa12fa8b4b959938261a1ec8e607526b7a279
31191":"":"fbe6b8af6685422eeeafc32327a99104b45ca5602513aed0a5c6235328e8a7a5":"04f137391e27caffecd441
3c775117feda27cad839aa900ff2af47c700034b08":"f185925cc180e556a0703a5956ab6d846121f9d9cff97f65bbed3b
c44904cb5f":"c8bbe16192bda74ef89d9859b248ac658896bd40b5491c90e923cab6815ec3d2126c62410370f5f44e01
fbf1d1653064aed835604d5fd0633c8b71cdde6c831cd91d69e420db83e6d5d82c26c47a11f2ede616a2885a884835cf2
142a6ae4cabe989700125df12902374bcce04f3fd78f034e50398d9bcf463dde6796627820c75a7efee82fe4e16375af57
ad3154973042e0a92110ef745f468377f6cbec5fa1a1470eac80408f8e96d37248b100ef8476c2a85cccdfca5696ffefeee
cda9e0"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-384, 0, 256) #4
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"e8e99ffcf08aad8e50386f5d079d79d3db783a74165c6126b42b3140f74

4a7c723541930c8c772adb62981dbef8d054ecdcf1c30228904bd7ba31798bfbbd64757aa251ac9a1ae8c20a050670fea
c59b":"":"546e04247d6cb5212a57b62f99e1cca767a5768cf79296f45f0db24732ba6368":"fd45f66c8dede41387373c
38674605f3e075c9b7cfc66123a5478b8f8e3ab276":"39911a79c6edbbc805a50d2aa018742094177a8e216d647c6442
8c00169ab2d6":"871577ddf34b29e5caf132aa82e1d2f1586b76e39aab62acd02f6d4440908a772ac5f6fd48c5f55f1ebe
0e76221ac46b834a8a4f5dd9958721ee053ba3aef1574ebd980a5da6a94693662717ee548af0f921421d1afb814e4d179
9d351889d2a1bdd57570a913e428e6613b16e158c1cfed038f6578920d60db73dc10a40da9bc363a0206b4e7e49670ec
cea866efd9a05bc237042cf052f2a4140f9377e3c6792b88ea06323fcebb99c643fc1c3653758d6866cdb148837fb0fdf7
7de1564cf"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 0, 256) #5
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"c7774e199b5a8c0b306ca236163249044ec2153dc89bd1c1459cfd40cc
6069fd1921837aaa80f4dff34a97b4dd7e94c0143efa24f34924fa52abb4275a63cae7048a7fbb8b76300fa8d109f9561f1
699":"":"1f437f758512071bd23d091c2b1ad8d51b99acc663e1d037fc5421092cbb1a45":"c622ac1071b50e4f899e47
60cfed476adc013b6ff95c9b7be671f79cd2487ba5":"f973f45f75fb0d68e0bc5a723a72e722e6c8f3fea08d785141c787
86da5101c6":"9475c697af430e94ed396c707bb7d5ee5bff18405131a0e898ed38065abc28ebdc1dc33d767c4dab69c8
46e3350bb414ef2d43798710958a6ff3e6b55de93c2ac31793a1dd4b07379e364ce72553323b9bcaa8839cbbbd347b4a
82010b78967219b84c6fe9f9285ff741a0036aba6bfa7dd0d5a4ffc1936341b0e2a31082123b6d2af6740cb3ff43bb4a87
ee74ef7eb06030745453d2ec225c8f31d214f1dead0f29af01ebfe90d2f8a8bf5e031242ebfcbd136b3e3db1f63a46f69a2
6d6159f"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 0, 256) #6
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"898963d0237c58e4b7b6e894ab271555407d3ae8c1c4599f5f5490ad57
01984a6e5ddd58d311b547f6fd2d4d67addb4ca6b86839b83978baef72b8cfbdd0cf180518af0e32e52ad4a73db460af0
5e187":"":"cbe5f14445cd310aecc97113232a0121ed2082f2c4152b4be68448f36c91b1f4":"efe0ef028e4179ae10b378
bcda3d96056ff21d94404bfe022b563cb6690ad563":"98cf6a771c05f904b53ff9b12709d20bc3f1821385cf27ace7a4a5
84e73866c2":"5682b6bd667b45dcf16527a817852b52a7f5d0fa8c962f3dd3af63e7e71990da92b75e9fcf5de59b1565f
525a734e978ba74dd80fe89a2e527960ce4207b9ca514d933676ad93e6dff5d57314a45889637a623eb7832854c3897f
aa511ed6dd246d2b8280e7d0524647d4bf7715b5546e0a9a1dec246b1680adea2eecdc354fb3122654102cd0bf94ac93
33caef3fdc369e7649653352739783d048e08e8d231b332fa1558745e2ce89dd76d1dc442a71dc3d5eb7d3481558941e
261f989b097"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 0, 256) #7
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"426bfdd4ead656611ce49bfd9f213843c194bb6863534ebc258415148f
457e6e685fcf539922aade348a2af678038610af676246632dd70920d661518d4dc5221381b2fbf1c2f3bfed01cbb9303
98095":"":"971785b18e244d03e25b9a80c2c2204f5bab6dcbcaec986342450eb9b376bb5e":"5de582cba43a61086657
8604c9f2a542831f41c277d50b324f4edf1e2e5d498b":"46e4c325d2c45e00a3c17ab35115b5370abbae61337eb2da4e
6aa91f951f55e9":"f2e8be2e994b74a4945fedabb167778523865ed27826f9c26ca2b49bf32af1626ae62bfeaab13e9bc5
2a081f365062a5cdbed0872f6479cfec5a5e79171d97ea898e8d10ed71203882d1d7b7d28c5d59b8872985abc628e736
22f616c4c0904ecb1e4518be8b4398662dff8806c3f43750cc9be95aaac2a4730f40323d63af157d13555d043c4d0d7cb
53f202df282fdfc5544a234f71121e893814f4bfa926351c5e9427e90f1117a3bce7a16f0e08cd06c3d7c458f9d07ca326
9e015733aa1"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 0, 256) #8
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"ddfb3d1d93e977aecd08efbd71dd48168e67658d93596b742670ed7c8804bd3e730d34a80ca1fb4ad2471ee22461bbda670337d675a17721ac63c3793153830a26b1871b316a3e10e49c555f44719577":"":"390c53a5ec1db52996eb042f9a76e45f0bca76ef6ea31b4642f00658342e601d":"b5436e880c15f03c3bb846d90f3ee5fc5bf5393865a112a4317d724738f5dd25":"d193f932af858698ab086bda36d04dfdbfaf487fae4298b38fef97bccdf63f38":"bdf9e1ba1fbafdb8f4628098aefae4810ee7fd565d0d285ddc3840f8e24a9985c2de57edf5a511079ba6c952c95c626e296fd62f3579ad03db536238fe69158317c9c26d373816343505c60a48e07a00edff8fbfef0ce69ed176e5484d056af02a270bb6fce7bae0b223bfd98ad359d53b159f3295be3fd630a568d2363121c7021ec23b14693be48f5b55e06be3d729c2a80948194b1266da96317bc592362809409a7666d5c168125b99de26da741f17ca52d63685ee8d8260d45764fc78ea"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 0, 256) #9
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"457e49a71da81a2a08bb19b97ba8e62ae4b5ad4ae64daf758a83a75506f9251149b2bd7180f69b9217346f8165b7cd8f100e0b1066e2877f5e5da21b037c2bbf178611dae627d9beaee64a9d0186462a":"":"c3181f694695c21405588f600ac33871b519e2b8e3b876424b32753da483d6ec":"68e717410f99ae13712175e402b51058b7625b7da27224414b472f9622d163d5":"f2cf13d05e853a13ed47c5d0eeb9c0416688050342f0d345ac1bb21d5ae675fe":"fc23aad02870885394ca831b72201d76cf736f08f6132b12178e8e3b016fef8d3bbb849e5d935ab732054ca701154e7d3e87d1b51b7392ccfaa19c4ad28638c67bd149ff67a93c09ee1fa5c2ef7bf9d40844baae79169e52e9990c93f099e036b63b000fb8ea67a13167b045c8f9163045beabe0575fef00b89fd90390b0124961698f4ad8884a1e1faf576de7a179c03221402279b31c93136b9436f9a07b5a67b1c199e7c6cbd0b5f53ee5bd0ef845243077c6eda0e021ac9219f6db5ad503"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 0, 256) #10
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"79e96cc8e77d8fe72cd6c66becb52753cea28bf71680fa541f345b83be79973db4081201bf23c94d1828e9ca1e825ac18aedc5ceb87a4c1b0c333c88d97e0f12d61b338e5ace5e15f71283d31a1ea90f":"":"4304ccb2666b227c92e2b00659ce0b34dbb53451591e32914a60d6e6cbbbfdd6":"d6e74777c02252b0613357b9a582f4d8cd7e436daf1674a663561b62d8ee7143":"0de123897d5f090b52db88e4c0f9fe736ccf27c134b0f5eac61b200d15e07986":"55a369d136e2d903c179472eebfc45ae236994669c46cd318401bc662f38a1f714f78ac9f15c819d2bd876a7af51e6caecff3c650a3e661e5d137a354cb16aed5b1554545bde08c10baaa5bce22284083b43a6dd9941a37f1a18929ced61181c137e9e38c79d107465a5a12f2a2f37788c8e398ac48b2be944d6dd3562c05922c25569c26a1203fdd244920e6c268028dbcf6807c05bbf1559969981467a479d7117a91f210118c1159749a1dbce4d8a0d5f2f8232c5152cbaa6441865ac3a88"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 0, 256) #11
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"b37180874dd4a7e08b1256966ed5845001b0773b5136956dca7194cd12a9d9e1f1dd35534f579307de11c1e64875e9377081de3095d83ced0ea3df2ee8d5be4daee545b431dc908bc10efc04db16ab4e":"":"d3c8aa88cc8d5b59af3685177cf3826cd675854deddcb9b501c40c4288cd9cdf":"6783f5bd86fe178e6a4d303342374ed32853925f143a5ad083c04a9c298feb99":"4774e5d062eda04b680d717f652d87bf5cf635f597287b76fc35e2d5ce593d08":"e478d45fd3eb6f4c398a0ec84f93ea6861f00666753c143506c5e417100077e2c4c9ece450d98c9372d68aeffe9e57ef9176d4084f9c6d02479b516942dd4792a90ffe1e4e49a8156bdd872f1f05facc06e71e581f919cd94fb97

208515ba284fcd255ea6f1d1ebb7d351e1ceea1cdee631072d3fc3f4ef9d5fc57a9ca98c88b81003d858cb5be0a3520c34e52d3beeadf91388ec9a495b1fc7ff7a6799ab0af211abf52c15467274c04bd104df14033df000d8624acd253a6c954c0d89b7238"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-384, 0, 256) #12
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"2779f20c02d086d30d53dbd6e7396a35e677214650e39f2ae83077fad70c068005faef347e7f73efb53a92f0629e012c7e1246d07b4e1bea7008dd8ecc7546e3f0a6e0e950e083373fde3fd994e114a4":"":"55edb840b85b391d4f1940be52a3e3824119349c780811c570d2c88dbefcea16":"e83ef56f09f82af4dd91a0b887d3f182dccd973435b74b7b3c432b39a61fe720":"eb9f30f2886d0486c5240f43104e426b36aae0006c4b9c64dab1bb713bcef7e3":"68c3feda06172a191184e0bb77a8f3c9096048bf71ed95b20cba1b1726660900d7d9f97b7ac648c76b50b921c28eee3d401ba81c8a46fabf82301fda8ffe9d76bd93cb275638f7c2088cfde88620661eb844cf953cc141b31e946338a0203c8ae67c2af1330a53251818aebef893010f16a519fcf22060a9aa9c597f3409465cf3c9ccf753db8c0bd3b465b028adfc447e37b5129c17ae9e8bd01f762662c466491fe57384825c163ab8a26d67efdda01b053c19d3bc6545c3661f2ad1df1e33"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 0, 256) #13
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"71c9fb2eb8cca98860f955a8bb3669c70b6f5374256da23fcbc4ffc2e90bc0a043b8ecbf1cb0c7b65a2cb7a47211541f2675512138964d0db8074727158bfb4f0d3c093f1e2c2bf697a48c2ebd27153b":"":"13b1d552e2c8c84f66961ac8c919166a248bc62fb896cff0b8b001cd7e147bd7":"27d626121ef579d9969809762c77068e4573af44b6e947a2892337a11404c133":"456ea206c38662750af39aed5fe0a39760f4dac85b83d7ccbc335f53a160a0c9":"464aee8af42ae68ee776780113805cade246b83a698c34bf4c92e5d81f28829ecdb808884bc7d784397f2b2f8c76a2e3517b53bcdc7257f44ec9357d014af4e8ddb44df98da72775567356f363fb85885f8f22505e5b5a80c824b4a0bc48029e3419d3d2f161b1469cead730cb123ca8387a2c8276635a91d0dcb2220797ae2702468587ac3a70b927625f3a6e2980d6fae6fddf4b380ca0d91eb4aee37b98644bdeac345f49523a241ca392972da02d70364f9401c21fcf39eeaf414a09fdfe"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 0, 256) #14
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"c9e54bcebbbdf44051e80b91cd10c87dc24267923350b6770406551a5069ea2255201f3f15bc3a2e4caaf0b45510f19db299a41db8d56ce993ade44323c455fb1a3f504124c35a9e907d9765e810c939":"":"2819b3ee279d57145ea1020ebc77c46031d69524a843158192e081f2ac91512b":"269ac853ccd332fef61330af7e80a33791ec44b6cbb83006e5ca0670597b35b1":"fdf031b1e0a8016bdf6a6ebb533dddaae1a3a5b14b9cf52a1a8028cc720b10c4":"a1c4c1d6e72dae5e4714bddf4a1cb8d01cff8a3973b12022011270c0de7ceb85ffb6a6aedfa54d0521ff33d748fdef8f29c52c7c414e692a30dfd0013776b58f58421605369c83d4d891a19c782a2d036f9638aba9e24b0eacdee87d4a8011699b638c287f0a12f11ede86a946be9c00d21a31584a2a0da536dcbf86e2df63be9a7b771999c9c7a6b748de713b7da757de2d731a8d980b75136b0fdc75ca7aef47cd36bb9370c5ca0ef81b9a04fdc78698720f68e5d54e1a777e557a1dfb4c22"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 256, 0) #0
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"4d95f31b9606a5f6d04dff1d89b50becfd0882e6cf51c1c5d24ad843bc12d977eba4582c39d793a63eadb63f292568c7fc4270e6c9aec83186a20819a7d35e7f1155ea108794302d593c53ce9d25422b":"43bf6f32b3b5f580b54179e4102d063536e7c47681d6de3cfe88fd8ec66e4873":"":"":"":"e991d000b24ebdf8

38ba11f9849591b0029feff33604bc4d71acd94301f8d045eeb1f81f3a101a297403a35859113c099939638680d481c86
067f54762892f82146f61cce7bc2c85d395348f3ea2aba6bb3e59dbcf8e41a81918b6cab304d44ea1e32573cd6936f38c
dc11d3c2f96290cc27b0dfa3bbbafa9394acdf2f4435170b428563427c4b02ed25924226edf8d5a5eca4eec4aecf98ef2e
6f75caa70bdd84877df2e637b7fad621c6170ca5bd86e21d0bb01cc90fe2e76353a9d5687bea"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 256, 0) #1
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"1378443dfec3c03d36b16bacc480edfcb1a4a509c17cf4b35787dae3bc9
1ade6c113a1e0df927a4449ff9e2f4f1cd9a27b07f57ccd6777f6d6bbfc9655f0676d7b4f91712efd43315be7c7f30e51da
89":"f67cd35afbc96756499c68a5ea19991cd1ad4880fdc13afaa817608a141e9646":"":"":"":"b32d9838b3f45e3c4b3e
de1181bf0aadab96d22790d8536f5913fe95c3ec0179dd1c7ae69430bc8c68f4f30105199b785a11adf7abec007d18abc
ee2e65df5a211adfda35fed8b9389a61d2fad33fe020119e72c782a316f17f8a588239567315bda461f5f4518a1aece4d0
ae028c153d67a8d4ce620e571faa0403c56bcaa864822e4d8ae6d14feafefccbe879ce4baeca70d436218e0eb3a62bf15c
018fd4cf66a50e3d9d7cc9e4744e29e9c945eabf03a6a2c4ca57e582b60914417da57f6"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 256, 0) #2
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"69e9396c58ed867eb52fcd046504922e2e9a9b059234cdd3f0a09eee9f
dfd45dedf5d3860b25115f8a3d0e2f3f543890a23a5aa278f836577956944a098d18f05900d1b076d30ea745be745b9ef
c0dcc":"1b6e1bb613d199a5e6f1b5c2ed041cf6f6633e2ef4d50ecad89b28102bf70554":"":"":"":"ee09f7b24cdc6b51a
8212ca00613633c1a5f044fa921bec31baf679f5ba66bfd723721a03e0f260a44ad5cc4c580080667a781427a34c3d2fdf
aceb4b040ee675491c4dd0c0d13abbe81336384806e37f2729e7fd080fd57011b54b664d58534c831c90d182d4d95567
6938d484087b0086d2bf2737a912afb66101575ca2bc5acf845f4970bb1ce4441eb667d5096319d6282714a8a9708ef9
964cadf596ac3e7b1ba18fdec7e2e22f5e6352e825e965a494cb880aae78477aa3bcba9428107"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-384, 256, 0) #3
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"d2f390fde0b50ea4afe6baf29a75e698fb0275c04c481df03910d238f4e7
2c6f63a6231df89123c2dbecfe0cb0313db34288f4143694ce2df2484d20884dbca097e35c3fd8ddee5273b53c1149bf5
070":"2bc38d852d1ddee2e89b7174032d96c0b97f955e16bc61716c5c64248eb6232f":"":"":"":"e62346c72ef393a290
4e982158992df4ccab03142c41d8d29c1454794926c48570eef34bd021d44cc9106401e9cbce6ddbb6c92257e89a7874
99d7f7a2dd527833307e02f44645ddbcb1303f1da95382c89805c76a2f12eb13d2b0205b7ec0ef21f596c98af608a2f2a
2c5e3534e01a23ba25bd5fcba0481482e1ec8138fb1c86840060919d7620cb7b879d1096f64aecae1ea085a793a9f4dd6
65449ce73cb3036dd5f2a49138ce88c461a0a9e2f0c1fb8338f5eea53ab0a0ca8a8df9c315c4"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 256, 0) #4
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"0cf86ffa1456c453b53305353ce43ad3ba44ebf4c6943cde8613cdc417e
e9f6e759c0bf4676f1ebd05c519eb84dfcd3e379ce61016e48cccde24753878f7d8fd5da72518253b2f836f32e5b594d54
ad6":"088c917f84679641f491aaf105eea0f02d0a8ae0b7add69645d1ef304c74b417":"":"":"":"79e71d9a974cb88d902
2d35997032bb5fbf8f0daff411467217837a836aa44c493f868a333d1ebf66689895b53c9e01d58019dd1da2354fb966c
88d2d6adbe66ac0b8901595a24dddba609478ec36e497f6fb6b4bcaa88b1e9a9c87088f66611446e8c2873e89ee1006b
6d92d2eac54714fc6481e7782b38ed4b18d5f9714ae6a544110cb6063c8a9964c52a7026f52af448783c3427092e0339
efd7d1a8522848a2faa8aa19c21363a537766c05505cb979269c73ee90679feaef8df13b6506"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 256, 0) #5
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"7179c434bffa377d9b6821da9571667c8b962196f7d8aad062e75b6091a34a454e8f4d14a60fb5253ae373cf50edca93b8d2eb2075076ec8c7a42b7adbe7723a6ba8b51a55fadb16fc3a6fe9da020482":"bc1c39e646afc1bb62685b746007148494209a419b733e938c1a5d02e2350860":"":"":"":"3093a2e1f502d44d8be4f35b386774162f0e10870f9cd34e3b9d4e77c7ec7cd10cdfa0bf8228be96cb5741f069440a6b6f9ec155d88ba66b7fa84959c53d3574bf1cf9f1561006c776223b881dd396e9e9830af2c1b5f7457fc45e823b411c5c2ba3b11219aefe5508f75cbdb5e40edf6b1f61453541ac98dad9ed502bf1a8afa79604261c7a89e78cf2941d520e0c10bed18820da6c23a5ed1c0dffbb04cdcc9c3284d400644e9365c995d8c99eebf444f2cb051bb62f231301d31ea815c338"

HMAC_DRBG NIST CAVS 14.3 PR False
(SHA-384, 256, 0) #6
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"b063333128a6ab4f433f151ae8aec4283ab6d1cbf4a69447850fa1a25930ec0f4204da52752a9bdc788c5cee6d8b92e1b8530dbe0c81b1d34037ee53f20758d5750d9863ed60c762ae2a8b4c973acc22":"067708b24df7a34811993d5c65d5348eea73e6c6680293afab5804b4328e7a96":"":"":"":"5f74a1d199f30fa22f2020baf036fc61b1cc2acaa80b48ddff1cf85fe5dd200a9afbd8bc51dd1829636fa335660f36d5d2a516e4c38e8ef0c3cad979e79e7e226b820634ef1d76ae81bc3e3807913eb0731b2e959c43afa83feb1d8da31dcdcb3dc3a4cf8f454c4ec41bbc822e58023f0d797c844bd8f20034b31d99579bff142cf53d2651d7a31b212d2b9d5705b048860d6c4e3f45ef1bf2d5e46433fec593b9f68be8b1e928ea04ddc4ce2fcecb737bb8f9d054c2ba5060fae5e5fc21a650"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-384, 256, 0) #7
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"e23fa0c86c8a7b99ba0d3ec3ca47349a57798c07587b666cc4ae1c9eff83b8cbffb49d1910bf05db3c7d0db7e27285ae9f6b4411d84364b27a66398f5b0a897ee2085526d3ac4f65e70800067d57a51e":"7ffdef21683a75484f6ac304801c213dc8cb7e3cf0f94c358a2e1ccc9969e834":"":"":"":"f952956cb8c528efe2c831c67b69e8aa7e79c013161497b9c55415fd40c7fae778a6fa82109a40dd72fb2f4d92e1cbc47f52d055485c99d893fbea1cf28dab35be1f162494cb79ea45c44a63a1685217cd3733dcfa88bb6de65c68f2390e479c0fcc6b398dc5498ac93002e7e7f360535d082c8e4638661107566506084 5c4f8bdee38c23d2f90d2b1d78217e865ecfb6df02498db837fe581c43382cd1d3a508b6dc052ef7c4d20349679db8d8bf8dedd763da8e5df775d133970be062a9ced"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 256, 0) #8
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"4889013333cd1e2b3b8c4365bde690b66e06bcccbea25f04132a0962f13a7d458e823f5ec0ea091a07065593ca44fe49611602d165a35aacb352206844acdf41dc2c88b63b36912ae81875bfd3e098e3":"b4761d82a93e17d8a0a461ec8205932edf218157459a25a7f26ceddb59992192":"":"":"":"72aa3601986e6c970b8c2253118b8381264577e391e48bddff0cceeb5101975391a2c731f5611316b255c2a6c0554ed6cbf8acbbcd8609e3f99c3cec38aa060eedb863563442b7beb78f35221736c608a933aeb0d4a7cc050fbcca351cf780d42c5380284a6163520a80896ee7f71d2961d7629d673791f8fac10bd01d32d95e8efbd65381424c378bbf54b532a70c285d98bdbb559c9f37d6eae889b82d5006fba2892ae16acab103aff1b247711ef92dbc6e516c92e388fda4243808f95170"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 256, 0) #9
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"cc32ef3ea3b0db89c69312cad56b1ddea73ba4c302b85ff3c6605d1899a96f49909c6a54d98baf096ea5bd46abc2535309676d9d6bb9917271bf8c86c8852e29bf3ff5b2fe56ac094fa35dcc51547

f62":"cb80942bfbcd8f112ed601cb12a5ca52cc0f280522db11da92ac6c76be3932fd":"":"":"":"2c972cfe1537bae42ecc
46b1b41a691350f6e63c202245347e91602b93a4cbd5c8829e5a4f63f7ee0e29adb69386e8b659dca2e6000aa03beab1
32db6dada8dc35ab68433671cf621fe4593018b1eafd3a2191507fe015e2a5694fdfe2c3182fada71d18c5fdeed0650898
62249c5508f055ebeceb9fcfe5d16e4479dc17e2b59b5a0aa31cf21fc6b5925569b0ca63d1a5cd268a4d409f1039d9025
56236fb06e61c1c054ed3798cbe4d8c2a7b2d18206212591174cec9da519fb876c583a20f"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-384, 256, 0) #10
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"142bff9332c48103221359040cda6632baa92cfbd1ae7f8b3d0e33d6a8
193939d9d20d17fdf6edd1b3ca9ff600fe965746b0ba1b61e9aa5141edb77ade0f191b87f0b33c0f3620801a755dca026
98883":"8dbbcf0c190783122aa6da6e05ec9d82ee29f8e74e59f8fe6eb9492fe410df6a":"":"":"":"2537a8638d5759201
cbc225e844208c1d08443b055fafe23329aed5eb2d814703b0fdbd0a89c2d62f8f4ea7746905b9bd90706b734060c96e
4e406675576bae84317bf36d8523babab72236b71fc6087dfcfcbe765de13cd1ed316f495e3bd08d780cd6a58849c929e
f24b41e9561868158046ffe8d2a89d169ba31331611f0872c6d075b9938e5170a3b8612f9ecff4743c0db5ae365fdc267
8ec262eed3b7c337e65dd1ff24a867574ee460bec7c374fc6b3fe9b0eb7bd9f5507ec5988d313"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 256, 0) #11
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"821ed44bd793a4af223aebf52413ba5e0e231b2029b3d71475ac028d8c
10f86d2382eb9c62bab540be847e22344704d339b798248d0bf2990c0621316e3c98ec07f05bba8887783adaebe8fcecc
48fed":"8d2c8cdb2ddd6934271941f071ea47dfab869a5671dff9d424b916c1ccabb02d":"":"":"":"a5fcf13e4a6b9829a
c30171920478a7878aeda658803f2e314f9ef8cf42c9c1933cbd8dfe5053abd30df644ca062070662f4b7e7851d28ff801
cc4b878523b4610891abb29c095a70665de1199182fa193439665cb19cbdb00aaf3fd0fefaa2278194e79ebf652713a28
c36f2cdb83f96c8eb1e85c9969381b52bc3444e8ad5d82c94964544b3e6649ae3f532d25a2e370e9fc8c77753239f1300
91c43720ffcd2bbcdb70a75223cfd9346091e8c056227f66648941552efaa5a0a369291e9ee"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 256, 0) #12
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"977bad4c5d1d16a2439863af8bb6fdbc206ad0bf20c4036c044645962c
36e2e853f0d702a54b70421a509c25de124f27e330eba581fc82efca522e43956187c9ee4f58f971e4b91ed51cc8aeea26
fdc3":"51cb91cb7ff1b39e18aacc0baad20443522bf869f26d9d7182005b5cb1d018de":"":"":"":"df4acafbe4f28ee47ac
c5134ef665a50deb68de9b3c7e075b26d5731049f13ffd00cda05f612f20fd901ff127277f269c069607442ed9f7b41892
711a72b83ac592048bfb28ab2c64c6b9f5eb4427450f4475b1c04dd4665998b638d06fe8f463e2f07ff46073003132b66
a5d4d19a65bd08230d1db0234fbd09a98864f8ca824e7a0ca9f1d1662027a60c7e95382122674d88224fb192cfc12995
2ed6515912aded9c72a49a39a00f9f9a16abbd361b20a12b5f3c4de54012aeb1b42f6fa3bc"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 256, 0) #13
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"3116ef07685eafff1c77f185fa840bb5627fb9a5d79f72f8007cdcdfbfefc
56bb1769991d78e9e48fca4c97b01d720d1d3ea6fa6ffbe2569da94b6bb36cd34d72c37d0218b3d02c391e0653e286b2
4b8":"f138ca3ec867cb7ed7d5fdb0868d7470de5f802fdb941dc400ad524d9032e23a":"":"":"":"59f01ec06c97a49cc5d
e469cc2b39c28db7612029e0e24e3c2b24f92c0af2383bfb9a0dccbeefdaec4bbd2607dc582ee7eaae6a4ffab251404e3c
59c95e5460ccc8d8dea4db73e924ccd7528708e1b6a9d62d485c93764686f93df6fb8a9ae86bbda1e038697b5485e27e
0bac9a18126bff1e7b104401306cc424e783f55ebe9940176d7123ef58c9460e5fb8311f745fdccd39ce552547adccdcd8
53bfba87aeb87dfe8ae72080fb7b3e5c4718e743c9f576d7752e3db1fdb29f160bde115f3"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-384, 256, 0) #14
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"f5ba27c487a40dfe342fe18e7f9c72bebc1ea229c7634cce87defd7aa11448e3f584d1769f3e76a017430e6e9bae6bb6c79170925e1156275311d86d4a03cfe3dfbf85f80bbd70ea98af76220833a0be":"34fd124aad5a10b852b2fe8481cd0ec46dc2d02ed9583f6e282a4c908e319024":"":"":"":"977fa5b70f4ca3c04b6f495de3bfdb4b8aef93bd14c82653e30a00a4678c602aa889766ab7caa434d9c15bd68bd14e66cdc609289a691dbcb391611be66c2056f8e675de5db9b2e2f15e5a330d00a8886eb8b8eed4076306d443ca292d783fb056186aa86e1dc9f18a113e015e535dffea954319cd26e5572f4173766207ed7d9b8b2c42a741340c1850a07139c0b358cab942bec51b159e50f5aa9d8fbe7ca9d1d2127a98fbf0f8c3094bea4e3039f7f7ab083fc9d050e29e7d4cc2d3d44caf"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 256, 256) #0
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"c4868db5c46fde0a10008838b5be62c349209fded42fab461b01e11723c8242a618faba54acba1e0afd4b27cbd731ed9d30016b5827dc2bfe4034c6654d69775fe98432b19e3da373213d939d391f54a":"135132cf2b8a57554bdc13c68e90dc434353e4f65a4d5ca07c3e0a13c62e7265":"a0bbd02f6aa71a06d1642ca2cc7cdc5e8857e431b176bcf1ecd20f041467bd2d":"93ee30a9e7a0e244aa91da62f2215c7233bdfc415740d2770780cbbad61b9ba2":"36d922cacca00ae89db8f0c1cae5a47d2de8e61ae09357ca431c28a07907fce1":"2aac4cebed080c68ef0dcff348506eca568180f7370c020deda1a4c9050ce94d4db90fd827165846d6dd6cb2031eec1634b0e7f3e0e89504e34d248e23a8fb31cd32ff39a486946b2940f54c968f96cfc508cd871c84e68458ca7dccabc6dcfb1e9fbef9a47caae14c5239c28686e0fc0942b0c847c9d8d987970c1c5f5f06eaa8385575dacb1e925c0ed85e13edbb9922083f9bbbb79405411ff5dfe70615685df1f1e49867d0b6ed69afe8ac5e76ffab6ff3d71b4dae998faf8c7d5bc6ae4d"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 256, 256) #1
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"46c82cb81de474ae02cccfac1555d06e5dc44b6ef526e0e28356ffc8bc6c0fd0628d4d942834b94fc977609c8ec0a6392c0693130c6215d55e37da43d67def719051e99871db68128e245217d2aa3230":"5de51e3f49951bab36460724a63f046e75f6f610be7405f55016c93a59f1890a":"5dbb13f5b4eb275cb757513e6b8af6fefd7c9c9e0f5304fdd9b4c0968458f22b":"3ebceff3232e75c6beb79d97c78e93244a257f0772f82e234518c50e322630eb":"dc64e5a1fc7b32f0294db138dc131946e5602266f4cdf00037ffe513a44ff83c":"e3480544036a3684a88e23ff41a4bbd810f827021ca45e800aaaa36ed0b9bffcbbcc99a1ef1f1528b4bfe39514c7a390ba132d1681138c4b1b9f1a0fa1758837dde35d0f6c38683ba47a904937dc5ee3d3b75f909e5fb6311c6cda5e1121edc774e66092aa1dbde83e4680ff95c0bbc2946aa4d46770f247caa7b71bdefac9641ee99700fbd1e560f9f7fbd462ede64e009ced90c44c6ff03b890e16c79c7b8c959a27defa6f062168891977c637ec22ecfe20601d499443f1fb0ecc7d9505b7"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 256, 256) #2
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"df8053def0260ae71f67e197ae8b547a228e9b67ba7909fc1cb3adca51058b15f6d5951f0b60c972d139b75dc44a3680127a84799fd7672e429f20876c175d135e5f894edc7a4da334eb8b73a334be61":"26890036a9b17d8e805c38568630e1c196091faad546ba8eb976f3aa031a8905":"40ea6bebb0cb94b7e527787e17ef9f7d3efb889fc1e47e49893ac5c4bba988c2":"090271c307b43b951c20ad3f081d2838df0936a4bbdc5eb6f2e16b1db482b1ac":"c203cc1a3af668e45653bab6b1aa39ba0669491a06d00cd39c97b777a8bfd4d7":"0d68d903c85c0172419dc9f782c5d67a0b3367d13cb2f734fed95c7fc082291edbf4fa83354c6588227e40bbff082be2dd276c264823a8f31ba18b00955d7a1fd612a2f37d824bc82cdec972d3f8384dfc78b51dca61e815766c877ef3d2113704c805a250aee7b55b849af048feb3536fe73ec4f0bee97006881d5eed8ea38ba1b8d16a3bcd91fda749b77d688997bff09f104a2d8cd8e133ea4

aa764b237787358dadae1c25092cfe09f79efeb8eb6e20c39cafdceed90e602f221fe6b1d69"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 256, 256) #3
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"b1a1b468e1d59716a23fb028e295588f17be6a79e589027237681fe9ce354860b1cc33918a64c8be171e595ee6a3b1ef46c2ef21df2815528482ab4c7a32449b97ac75a51dfa1c7e67a763f17e97bcd6":"77e5a3eb6ab38419f84b57997627c6bea79703c95bc1cd24ea73eba2edbed540":"52aa0be951816d21a2ede89f53913f6d5d70cc580a1cda8a49f8e49a6befa909":"5bd8e4ac61bdfe752b5a66cf2e048e812a8aeae8e20c3c8c43f31180e4b18303":"af5eab21e4dd9443b1b16f40413faebdb0e086991dd3c53c8a51bc434348311b":"d477404bcaf0ed53788354705f0fa9f46c4e2bef2cd94932b614b3c34e0b0c7c28d7483075c9745bfbd4e31e587fb1db77d557fcdfd3fea47da3f01e42635ed3fd87cf6c98a2f20aa833a1bb74a15b158e47841cebe53e4d5d8c85cae78ade156e025a7737aa9197b122e73a29ce0a881c7adc8ec228f4c14e56c722acb0165b1595f010266151801812c031efcee4a7739876777816af8baf4d29496912a012f1f33c07107b2db5ebd681722dfd76f3a58e9d7426e7fa75e326eaa416c5d820"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 256, 256) #4
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"098b8c107fbf943bcdd2199dfd15f130a20d518e95dc81988748e1f0ecc5c45f74622ca2940807df86fb05f0aab4727525f19d1d3bda1f70825f3e1fcb18d29e8e410616c105fda9324f4617af39f021":"220bbf23394c3cef156f683d05739b76f37538a0d360600bd52f0076425b5f5f":"af88f076ab39db1dd0e7002bae187965cd144382a3d1ca7b1ecd65d346f7c090":"bab9d09dce5073d11fcdf9539501dc998b6fffa8a0716edcf583a7d7385ff41c":"caf8d4e10513e5ceacad6f9f145a6f79e5c245aed4965ae85e2e7c5914f97510":"f556494b3849d78b06ae75571f0b9c8c108885fcb041dbd7892bf639d8ff6c82e19e8ce2d5aeb58e8b964ce4f75976a0a9c7f3ec8373b83150b88d6c58ff9b810124d4ac62d955aa64d194afef2f77de6994642ec86cee40aa7a5591e99a63edbd8bbdb22fc3c2506beee6d507fe34fdb4d4f525dcbe30b5747ff920a13f9e230899ffffbc5615e994ee96a1bfd8890cf607379be1a39d173662d0967c9dfea33b14d78cc8818c2a1956197f85e92bc11133ac4f7657f2db20eceecae8ca636a"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 256, 256) #5
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"f54e9df92752d30eec01c3756d569bdb39abcdedab80b0aacac76ab406723f480bb359a5fc6c7aeebb6719ab44114a75afd340af202be3ca30e4de794b826237105202dcff5d1291cdaf266673275825":"b69f77d5a08850a13f8e6d06847c4bec181ac0f6b720be3c06c0b67d44843c6e":"40f14c3340e7092b898758ea3c36750943acac7fbb6a83f0df3392f7936749cb":"5bcfb0786c447675032d2a32b304f25737de59cd07c84d3875c45475b15797d4":"656ab204e2c1834f346d89c37a30164db414827d83ca732c71ec71efa8182c28":"6eb8f276a8ff516f789d94d997f33c2e40b227776fae0681c83fde659462b72d37cd48c95899530ca072bf2470986ef29dfb193be7ee9ab3f8cde2317c9bf02a5f901ccb62bb665bc3a109eab7e3910888a522c765eb49b11d1ad0fbcc45abe3841e9bb4fc0e73188497cffba54f3ff82260767d0f70ea1668f45192e6719102e75aa5cc43084c50bdbd1ba491bb61ee9e5175092c1f50d56bfb68977a567e41c1e05d2d1523c198ded737079131fb12dcf847219d71fbedb5659411d7aff2bc"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 256, 256) #6
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"2cc330b34c976c859936c21e2ad88bb60ff153e41131567f58ad34bff5c9cb418939fed56356af7fe215986a5d0ed8e9a078dcb1d3fcee6b99714eea3bfcefb37a344a69d414965539ddce9df239be2f":"bf531083f35066ebfaeabd67b82d392ef6b121e7d9603a5407c5bc74cd596023":"51f223dc461ac2df1c4877f65ca876d635d50939fa9dd586c176d8ab73c6d605":"ff9d6807d71ded1305d9e2cdc811dac2d73746b001b53ec8a5509c4c

e0a07efa":"f5222c8966659974dd8a7244d2cee588b6c9a2700f338683fff9ccc45b6d3807":"981abda0e405c976435ec7f938570d911e5bbb32add52a8b94e528486e9dafae139eb15cc2b56fedfb9e4b2d10dbcaa5e6ab985be16c62b9b75a037684986843a7a0e3baabc34859253df2a053dcb0352a0554fd2d4530de0251b1b852d1d3b6e08548e215902ec8dc46ee89f3fc262c7a35aef8216b3def65bd56f0482a18a329f96863afd951307740fd8653d333f932940e2a87523afbc162c5c1d2bbe16f33a4b0ee0ec75bcfa6aee6d8348265938738be638f78506ab731d3e9ab345551"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 256, 256) #7
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"b4e5aad9bf4fb03ded64e4bf40ecc6fe2214049bd5889a5aeea0bf47be8670d329e6ed04538dd6d207767c367406d482ba7ad29231fd944f00b8d9b762935b93819ec62e0ccfd48f619ac40c9c208304":"67826d2bf9651404d5df4db84ea64dcab10697ecb90c68041f421452109af3c3":"67d6983465facf33369eebe0be12dc65fe736969e8f41478e44ec25d461e4435":"65f97c99140c8c9ba2ce37710b06f822cc0eaa03589157a3b575bc9c423afc3f":"19c37886d613d24b0592ea0b3a465ec8f8a9229abde3fb5e0122032e1ac8dfc5":"05777487bc152260a852e1b31a091f8e929ed22d8a652a77e4391abce7efcf0570df3d466d56dc51ef14bbc55309c6831655ba97c6050e563083fd1f2fe65b43d0cf8762ef6598d967b473b68c4143287f70d096a6ea120e3c07f2a95b80b393ffeafac2d0309d349bff017a49b9ea547a5776b5c38b9e981ed0a4825853cafcdf0f17269b9df6189fabc30388a383e3c28949625ef3d59a2c371ef416ace8658adc0e0b0104f1acd4b349b91b660d64412168d3c9e29680a5e324e4d0ab9258"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 256, 256) #8
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"27ae2120824f3d416bbea1f987440c507a4f01fed08a1be27e6ec16390c92c4f8dab04203543caa3981373fb991d855340c29baf439f23bfb599a5eeb95ec2059af24dd86c0825957ea8392ce3d980f1":"cd646b0d1971f249f4c4d1eaa17e60c311d813057e0b71819a503aa41e5c6b21":"90ee2d0bf06cb94190e6505a75d12dd77c266497dc99c5f89bde60be6789099e":"7d82b50cdfaab9b5d23fb6618b59dd28cf1a83c77ff2993d9f1edb87ed7bc388":"f7f728d8ef6af8c5e77cef1e837030a6aa5c12bc81423b0ecb07a2db95a32a28":"4b25aaf436eb600a103d3fae8e301d2755132b3de3c8b4c442129a88ebb3ab20c4d3a54078ecc4197994ff04bf0e460919978d47e45c7d10d76a1e63ae34624e2f64125ae1bef304efb1af688f20d8e212f6df4e11243a49177e4b6456010d784d0e4a94e75371a75c4050b27e48359549f8268dd2a2290ebde22282d96b2f38e3f06103dafae5f54f0019bfb013df39a76482ec7f878d26ef0e34c9c21e67fbcc3412aa0739e875da0e9ea1340592144eb232385fc7e605ecd10fee45524718"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 256, 256) #9
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"dbd5f508e8226acb957bbc4914ab13810b9b5b2b51a1b55cd4ac60f6b6d4c370963448fd323968c27d97e005b1a079c9e3ba151887006c56593eca7809b23cb768f5b3701b456bdc85fb5672a81db2d9":"0cda5d501072cf482d3c56c49a3c929b423f6e15a3e835888b3a9873647ffddc":"d3f38ca5c0bbcef46976c6a5965a8493f714aa2c8a2c817576cbc0bd6652beb0":"20014421f9af259892f017dd5392cc973f103d4736f3866e66329e5e7704e0f8":"686aba6c9c6c221b2b4a7de766963e4d9880676e7e6ac8e644dd273fcee519bc":"b720c7c56e10c9e436036fa8e1f1d1c0c0b7246c28bd36e5f3e88f988684b95a01127bc64cbcf12b9689f718baa52042b0837fea791391ee2ae42e54acc571239e5b654486a025ac25f46f10280ecdc65ed098e65e07dc3870b17af8bfd58edba026dc12b4ff04830ef132d07dcd7c62f67172caf2620a204869a81e39809db7befa25c5ed8a74b6d306c21cfd3778180d444bd99314a430ff4ef6b7061832df9b82603d6a0f646b398e7dcd8bb33a7926bdfa085a450d3de68c1e8cb2ee4524"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 256, 256) #10
depends_on:MBEDTLS_SHA512_C

hmac_drbg_nopr:MBEDTLS_MD_SHA384:"7093224d6bcf0915eb75360ab4bb789c15834a371baa24deeceb33f86e8bfb46f4e34325ddcbee671f9e45f7887c1481238993ec4a309e10d3f8e3952c840d564644062534f985a6b4e38688d2c800a3":"e7cf1f32ba369cf5545ee672cd6746ea9a336de7039ecbb25419259eabdfa44c":"bb186a460387baae27c11aa8c65d6ee003577eac47b259254a933f82ac683250":"d823535ed974b7ff9f19dc38b9494aa99f88143e3383b5a183ec00c925bdfedf":"56548af797f4a07ec42273f895822d877a311bf1f8dd5c96fd8449732a13a921":"159c6923fb71f9670db4eef12dadd143ee701bec9b0f76b56e9b1b8c473eecc3e38cf06c8f3b0c3d49580e49caeac0fd48da5f53d0d3e9c829c253fac4e4f09730177a63e0e759f043169e91459c9cf959d2230c7b94be168cf4fa02588d78aefbc855d55e444d671a69d274c66ad1851c56c0d880416bcbad08523cefa2fb384dd0f9f188e8a601ce0a92d42faaed0a299d6a9c86958854712427b35e73a0817193b50f3557e66d64ad80fa9ff87427b7de5b7e6312d1d9988ba77be90d4cca"

HMAC_DRBG NIST CAVS 14.3 PR False
(SHA-384, 256, 256) #11
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"ea96f8787458e505f5858e31bb85b6e335206f6d6d04bd9d333029193bd2a04e5f85ad152675ecc090119aff7720739bdbe34551ebbef10e822cd29e9ade1488c21fd9e798369d585d6f58168d509d94":"ba45df1a14e23361201a467d2cfb7a3dce3128069a8a59a9a388b8e31c48efb4":"d551272e5a60aa1232fcb4765e853de2ccec08941acc75188eca37120fa49aac":"c1b34347691ae9f1bf6be396e8b49aaedb38307526627399fc10c48748c3a7bc":"722c0efa445262f5800abf75e43d9daa44e3dcee7a7528f7313ee52fca9f1803":"e2f873758c4e71704d8545dd1eab51206ac11dfdb00dfd1ec9e53bdc7f6b57f5209727049d4d781059b0bc4b6091c9bdee947127b8c8f03f1ee5f3665720a4f6c6777682ef1937719052254aeb97e3a17b6b552bcbc9154551a7ed41d837a27b6c37b426508409b75236cc156dad89d896f25c54467fd45f9698a11c7ce01bfb1fe171e4d33faf73a30c8992c51a838e9c0537354371bf79146a79a6d42d4e987b9773377fbf384979690b2c04c332f22567fb0921c3e33088d3b011921fca6a"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-384, 256, 256) #12
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"92ac19b133398b7d8ddfba3c6046421b3618923241097b8f68b6c7430b6d232ae9ad8f864f358afa7cac72bbc4fd90f16ebc9c15913c11094bf7aaa510e6241face016a99ca08de6525a570bd1741dc7":"0517ea7410bde64edcc70df48f3c87f578b38b8c7087def16031e52760037df0":"439c97f62d6b7aadac64057c0003a41a44ee549f60afa92797ee7c9aebfc8164":"669d42f9901e029bce7584bbd22a13a74e6f6ba50441a2633773bf5ac745122a":"8bf3c1a08b2d8459df96d6abfa90725f1a735809da78bf99f7fded0230771804":"3b832a7f1df591bba571bf7662914b0e5a3b34d38228e377e4e7dcb4b9cb396ac268d71fbfd2e1a5cff4429feba36f55c7e45cdac49a5fc8a787292011c61f4f102bb9a5d9c8fe1cf047956f21c74987d80968d2e4cfa29bd92a35cb96dd372d9baaed8d31ba3462b42084dc1841a4042311abfe4b3358f56c9e0c69e233638d3be56d0d269cf110d5200759eceb63fdf3b0ad25937857d129b68f038fc73a842046cc7c45292d6ec3766aafbc22f1491774624751f2c50fee830e24a34a27b5"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 256, 256) #13
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"7a346bd6d853803d07844ca348f3c4837fce3e3a727f712223da248cd82db6ed4a9710cd8b9f2e7b593cca42da7b1a1285a78d0c764b24c3e4b21d25919c5400b4adaf0684c787326c19010728bc6f94":"3e8de39ab206ed166b203c97103059e6a9317d47f7a76bf4511829cc2e27a4cc":"327976aef239b20833d36b7f352e8e6570f8f325b568975a661b54b8ada49128":"9419cdf1c59abc03013d7d443c734aff57a6d97c870a03762c50b459d38f5e09":"f2c9c49c76bd683d42dd9de9d45a97b78710f39f2ee482e877e3b0844647f9e1":"24a83991f9455a0410213cc138696cf4eece7b2caca0a627c6ce023b7f912c115768ab8aad0fb10e35591d370e0372fe020823365b5bbe713417bc2f050cbf86fd626caf91323271eeebd5f2aae36fd0aced63779565604ef2653a0770fe4e42649eceb6089bb7662ca3d744fe178f5ac5bc20ce7a90325497f55ffd9b25c59a6b82f07553c080f0c45fed23ce47d972605a2f603b72d09d608548a04031dd2bbae9ff898201e4460479548d70b176e917ff3e3683e49f3330cfa77a25cc48fe"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-384, 256, 256) #14
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA384:"2d8fb8796d8a1764f8c824c55b880c53d2205559afbdf1cecda3dc2d05bf001e6252076dac013c7094ae72ca80cafce2cab30a160ce49dbd646710bc429c163231d73fe0e121f8cef8c02f70598fa853":"feea8ae0b299d5f79315383d938bcf9b536d11e036b28056bcbbc7fcede21cfc":"1a0fc47fa95cdafd2036eb5314e0f56266e58abb0f03b5e679638945b1fbcd58":"30707f376333df203eafba7fc52b40d8f1d97521a71d579c8b8457ac1328cacc":"f179c19e45c4a4f3cad8b545d116ca29e45f322580b7fc9715313be53f047658":"eaf7523b910b653a305f9122363d96e17fd22ccb9b6158cc42aceea40c34eac73e496827dd5fe4312f102ba6aa7aee934d1f41609bf3e14c29aa3aca210e3cabe70744a09f4c180f3d1ddf8be0b530403c5238761226f2c2c7ae29b24439afd65d6d5a0aa8daa11abce36df02ce61d352ab08965122e16708731d72a9fb5de071c20c6cb039273498ff1588c901d997151edbbd41870031ee337b38233edfd78aab389fae2bd280e4bc85d1bd6655269c3359753b17fdac502c3a2e871149fbf"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 0, 0) #0
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"48c121b18733af15c27e1dd9ba66a9a81a5579cdba0f5b657ec53c2b9e90bbf6bbb7c777428068fad9970891f879b1afe0ffefdadb9ccf990504d568bdb4d862cbe17ccce6e22dfcab8b4804fd21421a":"":"":"":"":"05da6aac7d980da038f65f392841476d37fe70fbd3e369d1f80196e66e54b8fadb1d60e1a0f3d4dc173769d75fc3410549d7a843270a54a068b4fe767d7d9a59604510a875ad1e9731c8afd0fd50b825e2c50d062576175106a9981be37e02ec7c5cd0a69aa0ca65bddaee1b0de532e10cfa1f5bf6a026e47379736a099d6750ab121dbe3622b841baf8bdcbe875c85ba4b586b8b5b57b0fecbec08c12ff2a9453c47c6e32a52103d972c62ab9affb8e728a31fcefbbccc556c0f0a35f4b10ace2d96b906e36cbb72233201e536d3e13b045187b417d2449cad1edd192e061f12d22147b0a176ea8d9c4c35404395b6502ef333a813b6586037479e0fa3c6a23"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 0, 0) #1
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"8802d43f70294f532d2af0be0852b7a9ef6584e8b1631845306b583ab059111c0a88cc670b8a827e5057b902563840b6ba6f6919295f2206bc8738eee2b4e7b4d3d492b945150c76edf466cdfede4868":"":"":"":"":"caa3a5f9822f497fc3335c3a4262294846cd4a6842cdb290a011a94b6c3c27a83622dfc7e5c9954e91feae5ca8034083e2fcb493e210e5caf31ceb63a7f3d59dcfc3a859dac5c250981f7b663e4ef7222eded353c7f42923c6c6db006e927b4b5f44b73e986ddc4176ac03a5ec619b3ebc923d4a6d9430e5b9adf75a5298e76a110d0a2a4e2f7841f900c4067cf7ee68c356c4f5d13be8885801d1e578ca4d2cc32d48b5e6303a0bc417afac033758f3e812693c49128e0db1bc9ea2fa2f2c45cb35792123af63f42dda3abc7cf8bf5dac17987178cc0a64b0fde5c9ff2012bcf57e93103f08db1e3a9f727e1cf753ea44d62ead2aa5410b9e37812c43d60eb1"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 0, 0) #2
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"a53adcd8c8ea16ba80a57d9a55955197ce0d957bc92d8a0b548bedca149d78ffa9dddb64710d5dee89f1edd37d8b55dc2f50bd67e4a6ad0f3a01947e3673b10688178710ba2e7bb5f3dbd826c792c9d8":"":"":"":"":"7f89db3d0d6cf7c5557b4599d7f4c8b5235c00c9cc393f734ad7ba98cb8e767ceaa529892dc30d2885f161f47b9c81dc2811baf12f120bb9458096c183ae35e198e1a50fb91f863c5d82b27ed10864dd6fd601f4a1fcb07bc839bda185a9b18ce45d800049bd2f41fd909a12eb2fe8ab3e1d2f0f1187109d61e2af6df0c5cb9fb801ceb319d0aa9fea918ae9991720e4d9d79ced8285774382a4d89001fcfb899a7c3fb864f1ad2debf5f5c39ab04496ffe383e9efda0eaba48325514b09a253640f386fe12fd1b25da3b2373ee14ee9f2ff06fe063f771624f538c0e5620029b9490f33e5e4ff1a9bcaba76005c829e0117d345b73f986d7c8276cb54fd87e4"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 0, 0) #3
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"edcddc13604e036f16687e36bb576cecd71b20dc78f070033d8b6f1f8125ba2d2d3efdd9f01a93910ec29fc4718420a21385f8798218e1aebb810379a0871b534e067b04d6ec9d523f7cdc8d45bed4d2":"":"":"":"":"df02ec9bccc25feb7aa4787f5f63a92ec05b2cc13fb92c20924aba9e1723436469c87673b8987ef19be99ebafde91d293ca6ec7c1fa4cc8902a57417338538fbf897772cb96085768e893c5a09327354006074992cd6a517d6c57c7af5495a3d645798eb1962c0b56ff0c8c98e18c0963e5a581230909981b301797d779703f31b264f90d6483eabd8a41fec8ea69a57befe1f53d470fc82bc35029a4d089eec7ca3986485a51ad1e56cdf2dea5fc3d39aa997a53a9924777eb6f3bf1056a578fd32aca125a74c8d24acb7b99c37f34081850712edf1b6851f0a5e640ae7193d3f49f3654aad3cd106e41e78f1e93a8a2d01acde0e6ceb3f19e0ab49f4bcbe40"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-512, 0, 0) #4
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"7ee0378eb594bd2ef129f35c9c1d87727c71ae472363a596467a2d71871863d8476b636e2ffdc0db70be5f7792ae8a8cd40d3f03347700d3ca515880cfd7962f8ce1dcdfc5ff134daf552f8c2a911758":"":"":"":"":"cc14c0e72f186392e461f65a0c0711e32e4b33a407953215941fc5d06279d08770b3d165d568b2fddb94299de2e7a6df0820a64e8779893390ac173801ef85170a52b9c0334b4fde55fe08e90b79cff1366bc43c0fa8f5f8206cc468987a38123bbe0d27e7ea2d21e6a1f02619b8c270a5e416ed50ff7e42d9faa2f8d383eda55899d85302590622ada9ccf5d144313e5df95688fd1a9c48ddcaf7af03068e11729aadd626761f3be1cd36188c89d08e3d8a090e7ecd7394077bbbd2c7e1766662ec882901941e09be9943a72a34817141611ef84c0f1848efdbcf245215f290427a6247174cf3a08e4110d3eea05bb85484f75e156e2fe5ea0c6723d3f8f047"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 0, 0) #5
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"fb35f3ad6b7618735ddd273d95b442a362b6822502a217e893be3e36fd7be4553cfde0edf5d9b5f15be9288ff78fd0c09ebac49e71484169170f343f4b21e244d1391f963112dc061075d9b7d26cd171":"":"":"":"":"6f6814f55c7e226adb7687d73eb4e9b909d47f4b57693ce2c543436318faea92371e951d5d338c06bd95f0e7debd915e2179beeca9878faf3dbeafeabe3c9bc8d6445f863649c66e9c3609b8a3d54080b68ce145b2fd4ecb3c93801c307c554513a210e49dee13828b20dff092de2f312fd60b2aa0af4ed7e564f06adea6b3dfa74636e7ad16deb19e95df71d2860aeee7532aa9ff2a08c768f1086abefb60d860657c8bd7972ec7be3740293b6471cc55262cc120f97c0c08de78b705068dcbb2d0c656ccb8e2c6e3fed199efc888492ec641d4a54152366dee96008a80794cb3b4f5a36a34d832446d03991e4374315c67c336aad317920b99f9c35a493582"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 0, 0) #6
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"a8db61234723da2f0883224563a1bc04c7b4d040a7de3b659dea0086bab7f454c73d1f918ff29e2f98cee562e05f5ad6f2781f5786228cf0cbb50d2c8d94a1307383d41229a90c0dcf142b94b704c56a":"":"":"":"":"0fa5fc008c56ca47024692ff55f500e312423818d1eeb77b1a3442058718885479b405767b879943e73fb16956ee2293b23dcb93cfda420a4f37ca5eba1aafcb8700cf6f38f2acac88698f1c0abea975270dd4436292c8ca60576690dfd9137080db2b3a42107ecea5a631ac413384a9329d60a358d2c58647eedcac164df50820e879374bc2e08d971bf5dc65afa33ecd472e5fe9677635a79ad58b489933fe9c1f992429e5d16dc954d2de059b70b8f170decd1f22c36b034e5f175138846901f6fd7fcea1491846984ced8b595c411a9f6d21f3f15fa5a073efb5f829f3b34d601aa91ed8cc433458692f44ec1930f3ac5781ea001a3b79df7c3e82ae5365"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 0, 0) #7
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"95d7851bcd43fc71cd9656737a0b05b5f83e55451c4672061230b9b34bff71c025bd51ccc3f4c2a14407d5d569d250b840e24828c319c1b7fe093e5551f8acd20167b2839c8d5ce9710532d69812b8a6":"":"":"":"":"358b36b4b7f119fafcbfdd619adbf9593048ed7364377752def3419b85eabd444e87d1e952c45f7c9bea3d29f845f297dbb48c2336cf44216fdd2e5c164c81ac688feebcf460910ecb8b8f6c3b0150195b2c7f1fb9988eb60c0564f0e089e4c269cd19414f6718120ad3742f96730233dadd3fb7d9e898ce38b5b8244b0af62ddb1e2689e9aaf27017ea28699d08b933f9219676a98f817421c363a526798833f9e763dd19341f56599cb594f274051151b87bf219d4b87b72eee5bf4bc78053a59aa5040ad334e08283e060b7b528a9089f24b287334070853c180021b50595e0fbbde18422127b0ef7efe92b98788d6e85683d97b679861154863fb0d4f9a1"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 0, 0) #8
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"ee7a62efc8403a0f988711436efacc44b5098f9a3526dac49ad9343c80c98eec51f064968eb37d1a8bc8604e3324e5a64a99315401a2df8d8935e94fea3fc5990107bae19af886415edd6eccc95ee942":"":"":"":"":"7e3a0a32d6954bad579d54f136594add6cd30628bdd53dcb09baa98884547bcf3c8e84e4c01b0660d62dd8b44ae6ce830447c5480f30942e742bde5009fa769ea8662a8bd26135bb45e5a380439d5b1b0114969f42bafe4d1d7b7c9a7b765573538a7f5917af85bfa1fc57710e10eb4a00062c176b93f4b02255606a110840bfbb9131aa290635fac52b260190e9172cfef947f152113ff3cb3de73e22eedfc44f143b9c23c1670a057cdedaec28b145ac2e699f366d5d695d1cbd258b59d4c88bd8d1062ea578c758d5823c43a85b5fe1aaa8f3e4b68092d4107d6b11eeb613ed058747259ff0eb685bdd42b9dee54c1be9b613a4ef672c4d31ff84a73f553b"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-512,
0, 0) #9
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"bf02755e4c3db98cd26c0abededb5ce360495c1a2ecf194e922d87decef4173584a3788dad5b308c50e7c0a0a10c7a42f3c7b2a52df2230cb8dc7bd71c35d448fc5b1eb4f903ec6342cde118ac284c2f":"":"":"":"":"ce2806594da7a6f27385593b14669b5c63b6a5b0240d150abf0ea4daf32574604fcdf10c4965a9220c285885ae2d2cc1de8a86796357741645964f102e65150d1106cb5b8c5bebf5fdcd5e64dced9e489c188b619c2ecf96e7f96861dadcf0e7381b4d628165da0ec5b7c90d369afb705c39986e4884adbe05fb7b74a9ba3b354e858697a1db531ae32ae8184658688012aaeaa4f69b85b802f5adae64f049857d1314c7532bd40043e61af47cdc7ec8e85fe61827de39c2f1825fb0253ee73ca2423544bb64f8d2afe84db5cc8ad7694e177468dcb29092b4c85d069ad7b1c41e139642076b8075ab0228f542fcd2a7a6340917f82b7e356e5652eca24b3031"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-512, 0, 0) #10
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"a188065c9ee936384c5572b0910360ecd984cd0ea926c86b269f38f1040d41679bf9a91bd4e986f500036cfafc583edfff1170cea9f22a3140e7f4d198630fa353626518062340fd2f5b0f6b4fe7e217":"":"":"":"":"ea19cc91d80d37b8f16388fa62fe8e1f114f32f2a6108140b60c1994432b18445cdc131b21c884c74d155aea2aa7f62c7ffdf128886cdeebb395e5b8819dddc8c7834475d19162cd6a9c037995e3f9381cd582eada424ea6b67ad734c216f8380bfc8f5dc0e7a1d93c406870bd64a190a670a8ca94dfc0c02b61365a1d908a6b980627af6bce02a42dd9dee90dba722cf6bd7ab86cc4200af93ed226cdae14f28e242c6f96db866631b258be010d47c2eb95f01fcba4fd71646e6db54947a0d4dff86a107e226b1e4343d8a1d233369f8b560f78c865426d341f5f0713748b3ac4031d3d84bb057cded60b11de44cb221869e42bb054127388740e52535a11ac"

HMAC_DRBG

NIST CAVS 14.3 PR False (SHA-512, 0, 0) #11
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"58ebcec4539f4af1b32a854181dd0f512b8c704fa47537096a769eff28c59165a18226cfc779efc9550f7be02006d83c230cd6e6909e301d1e99ecd1fff2b2cd00a56c7a684c8907bbb13ce3e9a0cbce":"":"":"":"":"6f4e86f309f69144603961c5366e4f9b16d10c10593ea689a8e7435a327d2524f4468813ea7f3248d8d4bbe17b175cfc40617149983928b267dc0c4db46d2c17fe8bc0764386758af1a824e12eb897feafc1c7ef66f80ffcd993aa016e139991cde8435ee6bb0de45a7fb61eb1a6beb76e012b848ea003f687537e4bd00ced37efdda66333b53a8dd5220c281fbf68bfd9e72285e78197881efc540da4c1ba80a226013a2d7098d34af4112e7b8c865af15409f6901b952fee4a474e4027051e1dce879ddf5e84f3947dc9b94119d67e6b48ed6fd6b1f813c13d3ff30e121efce7918533925f50c8e381e87ea685f993619bacc9efc0aebc884b450646eeaa5e"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 0, 0) #12
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"acad606154f6ae06738d67f517cef4c8dd8dbb2ea333bac9e69bc0a4cb98877bfca3d906739d442608bfe66ca48c3d7d01f7d410f46764bf2ba4268713ba76bf7026203e35313ee75add608509de867c":"":"":"":"":"f6621bb82d8830707fdcc6f58a7cecc7501a56f44c6ba783f6f8187b21f5f3eafd1f38ae780584ba4aca59466f6f5fdee1e82b28b5f8db4c4dcaa28f030437de407b5fac632c96e43a12d13b54901fb7c112daee2699d8256c6ee26d60bb267dfda2c6d6b61c9c67cd5a5b055a283fa02d06cbb8b9b1c3131d7decce4db61243738af4f6652bf2be23d4b49a1a7bfc711092cdf655527ee785a85e90b58fe478a462b65fd9868f821ffba56080064d74724d8c2f98cebd9eb8fc5bf13399b04cf1586334913e8e9232e13ba10f9f2c365e50154ee91a00d981d4fd7a4d49c3a2cc0988d4d712074918f11c378c40e762b610c9f4df3ef58d728a23dff3e035dd"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 0, 0) #13
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"d2715947b420ca136a4cd5c921b8fae20900679d87ffde5bdadc7b0fb532f35e100d8d0b59810bf3222b07fac3a3c334e4ffd96983e51ad04c2c5bb7fea15e8a03e36b92f487b314a191b5ae4862cfe9":"":"":"":"":"75751dd3463cc20d3f27e3ec085ab6fcc37285030fabb2a6e43c0d438c7d213346d218d34e3fdbabb3411be233707257290599bbc69512ad971cec2431518f38022816b9f794e2328b39a8cf6afeafc4d1f408f6e05863b654369dac0867feee0c17034d6d07ef22dd217f5ad0f1ef25ac82fce018573d0a2b0d5a924aebc5fd9c3eb9cbe38ae3d60e0e92ff800c9b108fbd85b2cde1b651e080e6625ecaeec9be684f1f7d98caeec9aa5e1445e5c3de6afb590fb3be3058b403df6c556963e98cdb30460a3c688485bfae28703b38a5c42454d91935fc7519e1e3b311ba117b1bcfd480c015cf8e535af66521cb35833621bf1026139164052aff6aa4e51fdc"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 0, 0) #14
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"e1d2d72e7907e7214cb266f1ef641395e54b39e8365304661b0bee371f3246528417ffd58420e48ec063de5df4462e39e6cae1b5f3a3a12faaaf39b98ee592c8d4f56b9d4534add5104b357d788c23ab":"":"":"":"":"626a0863321ac75e0b6240ea6a619458634a978245c1533819c97114e63914009c9cab732f1310f60f64f033b00729424228671f33425099820ab108412d460f32c0015b73987e937b9bbdd29e5bfb8dbb6c95d2b69fccbc26b060cf0a5dc0992fb0e76b38bcd64fd7a726714e8c8542d44b2f9c5d2f2f8cb370b95e086b07e88f492f51fe6c288d78b76d0c3a6146c9dfce53e76cdbbd158d2944dd10197247004954d92f6b1df4badeb4bb1c98d7d3da2054e3300f6d8dda8863422e6a042c2d84b2bbed6be88f0704763410771b3786d2f6d968b6c224e0cf535e8d02c178b2e0b90e8a7fca0c431b7f3cf41b0a7c17778fe8c2eeb442c910ba88c7c364cd"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-512, 0, 256) #0

depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"4686a959e17dfb96c294b09c0f7a60efb386416cfb4c8972bcc55e44a15
1607a5226543b4c89321bbfb0f11f18ee34625ef50daaf29929047870235c17762f5df5d9ab1af656e0e215fcc6fd9fc0d
85d":"":"d2383c3e528492269e6c3b3aaa2b54fbf48731f5aa52150ce7fc644679a5e7c6":"c841e7a2d9d13bdb8644cd7
f5d91d241a369e12dc6c9c2be50d1ed29484bff98":"9054cf9216af66a788d3bf6757b8987e42d4e49b325e728dc645d
5e107048245":"b60d8803531b2b8583d17bdf3ac7c01f3c65cf9b069862b2d39b9024b34c172b712db0704acb078a1a
b1aec0390dbaee2dec9be7b234e63da481fd469a92c77bc7bb2cfca586855520e0f9e9d47dcb9bdf2a2fdfa9f2b4342ef0
ea582616b55477717cfd516d46d6383257743656f7cf8b38402ba795a8c9d35a4aa88bec623313dad6ead689d152b540
74f183b2fee556f554db343626cea853718f18d386bc8bebb0c07b3c5e96ceb391ffceece88864dbd3be83a613562c5c4
17a24807d5f9332974f045e79a9ade36994af6cf9bbeeb71d0025fcb4ad50f121cbc2df7cd12ff5a50cddfd9a4bbc6d942
d743c8b8fbebe00eeccea3d14e07ff8454fa715da"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 0, 256) #1
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"0bfd73a55c96ecbb6104fc1f91d8601e7b57cdf85d6e6b5360920b4e7d
1cd02629bb1c55e637fae1608f389d179f4fd2650251a37ad27c2b5264b1605ed5a51df949086c10ece31255701733ee1
c8539":"":"15b3816392285fc665572c48a168068a10994cbe4ceaa1955f07075039c73b4a":"374241cf3073e2f82956c
76897944ae9c43907fd6781202b10e953c3aab1cfb1":"4d434031e2a2b1e1ac5ec98081be46d05de1b4d25e3b4dbc8f0
40b627f8a6f7f":"f4283abc7c0f40478bbf0234e2f7656b7c6d1d356c12a3e1f76666baa19e8a05fc1537bdd2fe855adbe
c4ed4d287fbf571615f415867a2e188ab60b3390053b27bd8bf4745887c93e68d0dfd01608d6b306af273b66db6400da
eae962882c4c6a19b363f24d4bd543a8bcc7935f078602cee1cf3c7b30343ae2ae0d5ab111764d719205fc30325b2f938
b4ec4d0f1fee2f431e70cb1aa1e7d826d54b7b4fc50560453349d2c52f09d6f5eaac72b5b9ca9b00142d45abc550eff26f
1dfb8229bfd1eb21e4567145d7ca47c84001abd7f5f5e7101b9941302929a37f2150620b899907f7216f3e2bb1fd028b1
96031692bdbc0d2769c448b024880a131ed98612f"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 0, 256) #2
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"da5589e7fee0a023e01a50aa54987c5b6d70503b78403762cdb53c9ae7
ec65f853df14cd7e30ba0eb703b912387469bf7f000e5dd78dd80722e194a4616aa373be2e093d23f2a4e7224b841ef55
0772d":"":"4c74a4655dcbebd1331b86bc224be30e6c3386ba844716d1a6938447ca7a317d":"6397e8fe13b3ebb08c0b
7ce460b5a149b23433e110b881a9c095cf24d236cee9":"6aba359faab473d0d51f21bbe7b2ffef3a03b64364777a48f80
698643d9b2504":"49c7ea8e2740fedafd8d31571a240f175ab5eb83b2104f738f3bdce41c160c19edf7b2e2c0603d9e7f
4f26f132f6b8bd8c61fb0eb391a5b4b6d23e3db20584e08be87648984d0b9f3b05c763665b110d58fba8d3b7c635a78e
d8f56ce05414b8bf4e0985e1ff0b4f55eda8cd516836099ded2b6092c9a1d532bba363e0811cf507a22189cd3d20ac6e6
6380fc8dde32dca54ec76130cbdc0aa70b5bf3b582ce1405c69dc0e26f65d91644c557d1b55ef9cd893355e7836efcf53
dac2d468c4909e1538ec1555c94c04b62448092f44e81be7c0984bec13a53a953efdc16d3497b1ef5fca39231feff486c8
4fa7756419bc909c8782559951d971157441047b80"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 0, 256) #3
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"8a36af663dfcbbece9653be51c8dedd7ceb125d59dbd143ab4c37f21d8c
ca464920dd161245835ed81ff1ef1d09e367ed43118910c2b62d4bb980d0e4305b07e8b321c5a04b46d4a7dd4611aa32
8543b":"":"59c96d6ec4e49b8185f275057047153ef626456085dd77a01cb89cda060bcf3a":"1492daff48d8c7c9e9e8f
38130b8ab2de6e02c6cdccc25fbcd92d8aff1fdc66b":"d2f40e7dbdface320825d0b766d0317f47c74fb55a5a325d66a58
34db70d5eca":"435ed803caf3e5c94bcf6ab61969bcc4e83f1cf7e73e481494d494faa9e33cdd890f112c89bd235d6d1d

acbbcb73fb1c9a54a4b282032cc01787bfa9bf855edd91180432c27d98a2f7983933140f63688ca595e7a9fbe38d12280
023d383891f0fb8ba3fb07d835a0d48f3f90860040718d341fe5dcc101b51243081563589b00a3e7c2095118c13b8784
b387c1d63767c3c655025021b0eaac886d21eb5faae0e35fd073cfef4354c7b7e4ea1386d855e71bce01b30151629a700
9b851fbc404731841bd24fac155a912d7b7f7a601bf6559e438367fdd898379b2864c548bc8e2c088348624e33c82990
c74f994056d22add18e611665f1b45913a62f90845"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 0, 256) #4
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"dda69dd5af052570a7cbc2fd378eeae936cd301b197d23dcf21ce06161f
411320566cf1f231111c1ef883a88f356d94f2ba7e42d84574f39ba1946450fe7394e5f3b9a21005d797dd03f27e0477b
a74a":"":"0cc796ceee78dfd667c309499dc4ca1003b2d923026c65826f280946e9f3f1f0":"2483640ad6b242e5c6576d
f18db137a3cf0e4a3eb44bfdeadb9bb650ec816200":"ed978c3f50c3ebbf4b70a75771a940f03eaf7c468e9c4e9af5f8bf9
f947a9352":"9bf785c4a1006da21f66ae308e6f23de2d1b01521c40404da9b605e1ff1577ca1d1300f0e47e922d02331c
79b7c0b1e060926564979e0ebf77ee3e1f54907770baa80ea8dedb7aed1948df550b6ee95f2f71a28ec2eb5baa76eeaf00
62e757500ec255369a9db75c242924d64a391af1536c3a9a6951aa991f02b7415a2ca77582e8d25bbdd023e4d0a0537c
0074f5abe3ad34d24f5b98aac29a62c1c2648eb124af18c619dcda701e7a277ff1e00a8a267392419dfc1fdde4ee865c9f
3744d92fb86b8aaa872b0142762bfcb7f9a45dcdf5bee93bd631b73e3acf9edfde744e7492b77fe38adbe631e7ffb2d170
8f213136483ce6845398409b8550e7467b6c"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 0, 256) #5
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"346e27bad2b0c0029148c5db5419a124583d2021fb74677b37b13e864
3ee7aa9e9bc52f5c2689ae2bacdb7c8c8d22f5a4bbd2f0ad3479decf2dfe2e9312dbd682d96e199e07f5fd4d22deedd83c
77673":"":"65262e1bda7014866794713ce6bc1ae4f0dce523c82ce43e6e0cf9a64983964f":"c68c54bf2cad027cda08a
3380f3bd525e354c4288a7beda1a7ed8d62931aac8a":"cbd0049d6546baf0a8df2de5f15b29b77ad07f59b4dfe6a872f0
bc1cad71771c":"b8c344a8004072f76582e494f70ad0f7d21fdd13cccc387622ef04ca03a0a14faddbcecf8869e0f23b6f
13fe58d9d769f3ac96ab9b9967150fb81cb5d773ca44960e9267e858ec9df23228fe2dc239caaff0f948d189248f5c075c
3250270af7031dc0aebb327b004d84d0de699f5b02da1af448df0d13ae19f77586db22ede3f6d3d032d10ef2d7e2efdde
2ce66a8bdc07126cd49241faff097d1467d862efc2a2e198e74b2e3293d4a99bac75e328a1dea3477f3f4c95edacdee48b
14d26b054b5a268e242a2908449135825faa7b4fc0c9c877ffe7bb90faa7c3f136b2b4c78fad9f44c829bbf7eb8f747d50
1e150bedcdf4cdd6fcc86fc409a21e6e90e86"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 0, 256) #6
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"09587ae0ccf5c580b44e390e68e6a0a6daf45e7162ea04181358285999
18ecef9abdecba73d8c6d56bdfe005485be3b1ff284a85b127b00185f2f935356c3f87d076599f6b0fb7f93abf45f0d0bff
b3f":"":"4e703f5f59cecd926fc0d94100d1c54fc8b19d165bfef16437d7be92802b38d5":"59ccdafc72e5727e303d2284
b80e9224c95ce5ed0edcd816c18a55aef681b203":"36d72751e4d6a7c6cb2ead12eef191254df53622f6c0fd1f33187f0
9e87880e9":"c1fa1565591a1225e0a61e1caf0fb6e4c17740c1b1088f47b90d91a0f99978068c162f14cf82a1ca936ec33
12ecdec2f4b7944129722657ae20055a0c293bb678771b457940df23fedaa69eb1c1d487af7c7790b4359bfc84fc83e9f
64b81b78b5617d8074d8c7fbb443d3bc671f8d2bb600c3fff2231e0d363b41f3f558ecec02b0f1d59a63b39f5b82b59bf
88a0fc9a838a802875e7bbc06ecd0029bd62796e2047df49139bd5c34ef67dc930b1811428c4b547a6f67404012a5b97
f93b2895dc2c2389070220a078d2fcd8244a241caaa98a9c0c7aef60fc856c61a3b8aab46ffd3f0cfd768d6b41e9714969
587cf363b3ebd60c8c331435e9cd79430767f"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 0, 256) #7
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"1ad037daea8ae2b9131f4490ccb453b670596978e097c7b2342c5ad8bd
a53de10f696e07bf91bb091c21898a1f728bf5873089840b5f022441b355f8e5cee75917400c5ca597d6fdb8f52874cba
1ffae":"":"27b4177957fbb40bccb4832fd95be75ed8df2307be3cdd692e8878bad14ca8cb":"c7dd83bc2e99c2428bb24
3c35e2544b10857620fcdf8964b65b62c58b5069a16":"ba57de1455a25c66dfed3f8d2e3e198fc6ebfd7927f590c702d3
a5ae81e80ac9":"76957b10f67a690c33d9a5652514eff7b3b5ddd35acf424d0706725d331411f6cabcc35817e3dd1b51
053de30ccb0210bf428caf0fd6e9e798870e2cac024643f5e15f6c5591e921e7531e60c402bec732e79f55f354eeb5ced5
fb74513ac8a48cd6dd92a8f72ce26d87de25ffefd511974d629d17048f10a6315d1e06103f58f8d3a04391239d8b1e58c
bac3eb7d8ee4fe9daa194cddfaf891a209f7e3f703a4c18fe4734d532d9b648d55d92d6ccf7b1cd5daad9ee400a52bc464
ec300e4dcaeeed6ed9d741be4c548e45a6b9c7f73fe4b394ff285b629fcaf031a9ab3593d5358428db60850de0a2fdbc51
d5c63f956d6b6625207e2a0e401891a92ef953a"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 0, 256) #8
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"fd2d1b1f4150cbbf6ee3d8667e7f508b341b3c251c8b0abf3178d2fa5a8
0ed170a15bf55a6570f979080ead216effa5802b2e7404ad93c5cc41e17eb78168859388738fa935d1cd6b06422867a30
b552":"":"8937c389fc1b905660861a4062c4e6542cc2c587284a279cbc86c432edf541f9":"c1f79f883f51e1de95afdea
8392e121a9591674063411ba79b098e0869dbce33":"0ef847924d2fffbbdea4f12acd441e52ad39ff291e80c7a24802c4
f03f09c8e9":"26a17b546d2dc3b1528efb53b0b0f87e917116f03658ff6e6fc165fb891f483af8ede7fef8ae44ab9ad0796
1b4a22f50fbdf1714720704de4d80edd1b1fbab4443e961a441ce4e7959bae558e333263f79daff8d8f9e3ab0d73eda9f4
d3e31d535c67edba3d788ea7250584694628eeb55df97b01f5c70b051356b5d089b0a368d98bbac36c690e188e58eefc
9b5e2b59fdcad05b71bc111b786512d13fc0ad4b9f799287f03198a53b8be4a2183e7096a0b9fde728dc409414753077
e436fe1af94a93241021de8778d65a4708102a49875416170b30a6fea290d6882c41ed8c838388cbb7fe881a4775cb32
3de353032c6e29aa057bf81619e1670823a0ae4"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 0, 256) #9
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"d4f64d9c63708f9294fe1b1de82e160274dc7ea857f8ab6f4ed629cc5c4
fed94bd2ca16570134810e71a3a7a38fdee4e4aaf3aa82871142efe6b7d7a4888b4f0c745bdf649f6c84fe5a6519ace633
6c3":"":"a8acefe33c7d7933ca6fc3c8495bb315bd4edd94668084de3a4f742ac5ca1fa1":"095006f15ac6f8f649ab217df
add426a60ddab70c114cf7d52f5e6762a47e679":"9f095084b18d6eec18bb6ba7ff6a876344f0d6d7916c10bd510e2e0d
546c4a3e":"3d3e2d085a23f3b08c0cf1e49252858855f28afdbfad3a58983b1d815b2643a968de890af8f3d804969d716
dbaaf206985d413e2534ec6f2c9e144be0cf097590e3de9d63d5c530669d1b287f99d769e7fb6e2c71973c1ea02caf49d
3e400bd31d578313d5c73bb52535a86b28f4252c8f6bbc9770554e294d0181904881d5224cd30bb95d85a952913f63e
2bcb2c9e24e9a999a6c7431c5e6e2d76e4ea64480819ef95f40b72dba0f841cffc67bde3c9732aac9bc4dfde6e9789487a
b9e2fa87103155411eab4c2e9b640c5ff417307467ab7d9b6036c8e81a51670525f1ca234fa4ec23abe6dddeac0c029a4
b58d2fc8c24c3f57e2c2081137c92fdc373d23"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 0, 256) #10
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"f30723bc93a3fac546286c2ec8faf54498eea6f8d723c32c7b648265dc7
5d8dc14634281f7a7d1870208bac4896e22fc72bec353ce3bbe4fe2672c0b9f6266408008d0d1fff6c9c797e93ccdbc72d
d95":"":"ebc2b572f365a726531b3ddf7344590cc5f779771134ef7bd7aec4af95bfb532":"0941303cfaba20f7c7c4ee74

5ec65be3c4f6d217f8e6c9a1f5e6db94949645a5":"6039cc999268f1fdd5ee2979e76b584b85069f144507723e2a47e3a
f1d8c2355":"eb7797a46743e552e682c0c7ff02e1a06d5aaccbd1a54075cb1a9332e76570d6aa5dd7423dab5f12b1bbfc
ba8b6396f2bbc5a1bc4c7f1fc306b32037b503a1a26b509e7c736b035108f90e4b3ae880bcb1eada72644119f9ae9a73e
ada21f9de1d2b1356a90f83c6ff97978bdce08aa6412535b401dda98c4ce72534f6ed75383d51922e0a4763c5903baaf7
5e5baaa355b3448e101ca3229f5eecd346f450c2f2b11503bbf23bf5d8f79392cf1425ae1cbcdd5bce53ca7ee0b59647a0
a4b8cbabde28a7368fd46965ec0f55c8cff034ab3b733d19ceedf2b8f38e541da2bbb51e04cc5506d1ef8ab0ec3b43c34d
ca722e830d745ce631652976dd6fd9a6aadb"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 0, 256) #11
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"070a6da7f4f59da9ecbba2daf690ee9ad0c9cad330600b7ce7b95d5c133
6c96b47bcbbf8eb4d8918cebe861e959d68d7e5fa7ce34adaa38de3e36f425832e6bb0a23fe21d10c78800506d9054766
ce52":"":"3b4d05963c2fb8315371c2f35f375b6e39ffec667303cd96642fdf6ff5f99102":"4189cc93c021bc2f958daa73
7a17f78c03ca09a1a4a73faa8a74f3f109bf2800":"5da2d3a69f10cf9a2f5276d3d54bbba4ec02826f6ee0440608ff4fd6b
1ec962c":"f8d6d5d7aee571a9d75923c6a2ed73f3e77901cb025d3e609c7cbf83b6478899b410756f66546bbf38ac330
9f02fc870e056772e56abe76a99a147d12f1fc60ef50cf87baad21f5ccdb43ba43ef0ed777be5de30ca312f814ff05ebb93
bd523716b8f8ad0411aa732d2116040d46cffd9bc2e463664433ef1f7fc56105b393915106d8ae860aeaafa934975d446
ef95d697e1761017bf102e9e175c7d6d3a3aee0ce877f1ce7709d08c2c84a34d85d17f77e06a5f72269c9f18f94a9d9e63
5ba1a1b62ca5499e717423ae4bab477eba48143028ea7818d64563bdea3fde587daefd59fe7059f4f6db16a6183787694
6eebcd846fb5acf07507c38410e2ac3f22"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 0, 256) #12
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"09b75284b738d600dcd3322b91d380db45d3efdf2dc8e9fec64cf07d7a
606531ab41f05d85e3eed5f62d55c5132c75f151437d4f93dcb41145b2f95125d1daa7dd1f75dad6dc32e9e42a21dfaf3
5726b":"":"7ebffa04f7f0c939e1bfb4c8686ebe4ffd7a1ec3fb4aa114946a6650f2b449ea":"8d9ccf3526b655cb923ae3e
1416e84af5e458a2ae4bd55aa98e900353f8bce65":"d78edf2f7211f49b70db778b0fb0eaa217860f9197ad1242cda264
c3ffa3e2db":"1f802d0a9526017a56c43ebeb782c19143571f979b141b644612f0364cb5531f8fcd527578cef89263c6fc
5ab26baf136418fe203dfe3113124363c768812d3e60a66b14fe13c43891e0756fdab6f8dd2a28cf9a6341b7b39d99635
3cf435726b2a02560e0b5f8035c2a50b10de41ffe389f0b0e478d783fe8da8d729f1a7b41e09d3e3cc5f93ce24ad76b565
0ae61701035d2abfc05bded61afb36dfd910be47c8788af1f74cd101746207722ee2761e54742d8f21884794fa9b07126
45fdd962ca5cf2d3070f4a2c1db6f4c1aadbcd415486735ea1bf6894146e09c6cbdab36d282e20ce0e840871a0b435c3e
800bad673754cae50ab4e7855e268d9bccbca"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 0, 256) #13
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"773a12318265c2de4d6a80ce936d4c8a13d81b646fb197d7ade8d8dca3
8988e6bf4fe25d32c137ff50f5e20e987ca8c5c7ca4c2bfc9f68c1a79e8a0f9bf2a1dce0c09dee4134b39f1e51f0bc10359f
ca":"":"4d995d9addb816122b70226a068c457ed4635e7ac9ce41f1594ff84160c1c06d":"f068497d26966dfdd57d5a8e
a1a05c1db2ac2d72248dd59d17bca9c6fff28817":"641d5482fad78093210f7e542f45a8d17fdc856be5860c45465b077
5bc45ed7a":"4d47fa06ae54f60102bd242309d5366a953e72a2622d025f9babf6f6343429e4158691bbe3629e701f07a
48ed239e734a78a400463139cbfeb45d6515bb690f1211ee03e908cc446abcfed29b955b92e7f9c3aae149195e174d34f
10e30333fce99cf362c5a42a79ec907d90fb5806c1d09c9690d4aef060f0fd1b0b1877ccfc377dd675778adae40e87588e
5080d3cf3eb1f710f019611267b2249007a01b3e6999a3bab294766c933b09537e99ef7251c588728ee1bf8c64ffc64de
6a70a521eb745b4ca6307bd24ce5661def1d7374afb1c44a964f14edeb1fe457465c0b45d62a33c5c5bd1628d528b201

54d73a946c44363aaaf20dd41244fbc81dd0475"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 0, 256) #14
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"eadb3322979308075d4bafb69cafc6dff5d55b97c4a73dd9943a0a9e4ac01b78ced5ab91508b9718f6de9da47fd7bd54797cd5a5f6365c28b1a56cd5d74721afc4424a7ca53ed8e97a2c15a727a682e6":"":"8ced860d74040dceedc0fd0f3bd36ecaf36f91e4c56372ed1a54d25d65180d42":"a19980a1c86e9ee4db41f6467144b0dff4c0692141916d46bdb7c2ab79992116":"1cdee366e7c3e7e853caabc4320ca2b63616ae86343fc5ec2a21b6c24c04ec39":"84432c3f00ad23bf1ba4b464ceeed8da0760319141c214d6c31344fead11011ca1b10f19de5a3514c8df0b69fb85e8706db272d0e1e6bfd512cadcb4df7fe745aaaaa8fdd6e194c38b063c030de3da53ae6596834b99a46ad205690511e3aa69cf5bfd9ed78d6d33e357524dcc94278b127e89e189e52db00b426499a388241e9455deefddbcd3974236c67c6207a6f9c4c5d1403c02c828488e705fa4f85fa2771a1f3df7b2d5d4b1bd25788b8e29c679044e557ae4cc5dfa86559b6ec3b5a314d4de8affd2d576c3cb260413403e3ea439ed4df3501acb85dba98306cd7055027c7bc339878998e23f70680a855479060186335217dbcb229cfc54b66130c3"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 256, 0) #0
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"97aef935ea33717e8e8644bb8c4789f375c48a945ded08771149e828a22dc86682580f51070ba1e991d9803f51fd9a6f63cd91c1ebb2caa15f2837df8f35cbb6fe96df2674a136990a5976cbbab63bc1":"212300f93899ff7cb144f20426028b976380a348253bcc3ff42b528cd1972549":"":"":"":"0e8533f64b60c23a2655827037db218c2fe9ce430fa4ed6ed9be349c4bdc6f40018b42f486fa04288b3b0c62a12812e76e08c76062a510cc60841f165869efaceef90805bdde2fd66c36c38a2ac9c3cb86bfd30406569e0afd245102f2ea2d49e4ee5f69187227a3f0edfbc1259cb6564a2d4e829b3fc3b6996e37546f1d8a16fcd8201d1ad28661bbb0012daad55d5403e833d8a0068d216c879bcebc054df0c9cba14dad4863ee1f75b78bc488662cb0c91ca4fdfce7df5916b4e62580902c601be706dcc7903858e6b9920735bdaa635add5c06080d82265345b49037a32fcf0a7c9ea6069e3369f9b4aa45493efd7318da2ae9b4fc300498248afaad8d49"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 256, 0) #1
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"549ada8de63982fcbec1d27162a51764dbd770f1da46d87759b2ced52d0ab2e8d1e8b2883fdeb221380e17ea387b3a065cd6dbb671f1caeb7b5a4bab5b901088f081afcdde5ecea10acd810735b95532":"0e7f0664ee95e3de9ef4f9d8faada0851bd1de3a3a767f85a74ba26f7fe8201d":"":"":"":"c876001855484b73dc46babd5700139934132l5f6617ce71be7c77a418494f77adc56f5c26b393de340a514b40bf9a0a9e2629b768ed329ca083dd4af5ecd6f45f878a55d5b02fb9bf3fe043ee9e7058acb83d3aaf39ead7e11d82725bdff8272d7a22cdd6efcfbdd60458235e523ba0ec1b490994fc394123fdf65d72ada39215ea6c7f8bd6c8aa4ce947988442c66cf53f196db401e275098d9260e2162f5726f0c73b201b61fe9f7b586057780a87861d31ca5b21ba62eeca6f5387c5f42147d55a61e1c7d39398a82ebbcbf4f153962f6a6bb5461d58476b4811051ccabb00cd9a78debed345c7e854fa064f990a6d0dc827c39c38237bdc5e9b1b44b6a3"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 256, 0) #2
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"d3f2af83ed1071e6895b1d57d0969ec7fba3d6316df5031e452c26daababdabb58107846a2a6921ce3502614ae6cc94b9d246a8ceeece6a9cead94cd297838ca96b74a88dcbe24000f8eb719f939a3bc":"0d4223285e53c9e7d743dfafd08fa75c81582d0c507c38cdaa6fa1b398e342e8":"":"":"":"9b83018fb5a4b2d2b7

6cf5e8258e7d3f6943a494a9cf7dfe16f9c51beb6d9b849cddabfd597fba42d6fca4096e458c8c0e353da4fd6af9297583e
97a910bcbf1258a83da465d34ad13eeacc0e57f145a8cbe09ad9129302e64a4d6cc9166e3576d256b7b3c64540100ea4
b0c6f7f92ff13af732f6fce6516f2ffeccaaa0af906d4efb8b7625cc91c5358e5fd292de159dbac1cc9f0afba62ba7d573349
1538d14467f9f242fa66e79b444f38ca9a6e7472e41cbe8a63967b2e9ad0d8fab4dc173a3bb45e3654ad49d8d8d534514
6b33fc55c52e201fd404f7ba64c331d92c3109dd8fdb70116d0e84304772217ad8fe65bb0215eca5c842cb10d591c9b8
87f0f"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 256, 0) #3
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"43de428b90ddf2dda3280fc3628c289ea7e623b63a0ad5f568c459eb7d
62f739c106327c0f3a8f59e5bed661224e433594f78b3604b10fa048e04181eed885db9665c4eb92d0cb82969a1e5dbdf
11fbf":"e9cf65c1c1d8d1fb07a0a66821b810fe8893339949b50909fb9b72883a530ffd":"":"":"":"2698a29124c6ac40f2
416778a54ea080014a3258211d2136cc82e83e199243e7b6483f363ffb637e3a498ecda6926e91cfc19e61f66f33d3c83
0f2ce9a9379f3ab5eab90001a06b7713a5ab5c5ed461d1c99824e1a506482fc04b6ff0129847fe84b0e36ec7284dc028f2
ae326f39e7b2b17b6cbc21a29f1f0c8ea069be5a2defa5794880fb37ed129849cb4e7bc998a80e6bdbf6ee7d7bd78edd6a
7ad415e571da42481f00a857c57308cb7e24efaf3993587d3991ae41aba97439f5e0feb5250013d84619fada910ecbc18
6e976026b1451b602d20e60679e78c8940b3c8946454cb0409a83c2aa7e2d1f92f548fca8d089e15c47a2c803e7e1e78
429fd01d"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 256, 0) #4
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"af0abf3d221f4af4a4571eae06287c994beeffcd8f5df5da72eab03cf108d
67f71b91ff2d70698a8578d058c181bfe715d244f5321660dcec025897d9e9b037bdb406bd97fa9c3ce5e6d01d0840cfb
fd":"7ee295c84488c3f5d3b2798777f92afcfcfac175a937cb50444831ca60a58650":"":"":"":"e570a328f4aa705f4060f
9a6ff38e16007e59533e1d94d039c274d105d7bc8c2ff77920748579de5c33c1465d4441332ba51d30bd8eefa90ae8a42
1ca662551957e1875d6515adba50a0d297640248e0a83c032b515520220ed880701650c97727d6b5e5f9980f0eafa4d7
09bcbca76d31c291750f52b75a165023ae40ddf4ad66f395d4cfb1f5a5873743031d2ea2a093b2da4ea175bae45cdabe0
0687524a3814f153c514e1c3d50abaa96159516bde73878a021b2e9b889c130cb3d016560aa9ac1ef2e4fedb67abbd2e
dcab3d2d74de3f8e9fb1120473687902fabb46eb183d74f22e5b3bfcb9dc1d1edd95360ebc1310651efbacd0e603b3784
5f2a9068"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 256, 0) #5
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"54c0128113a4f3e76311736c83581e6c3fa45659c20bc622132ce4f9dc
c348e76575da4b0142beddbdcf51904d1febb248a116378bc69acf6d1b4b25d94e9d76145fea73f8bee448964486c39e8
8034c":"b147253bc1d28e988f99a53a73f5b86868b43c6ca73ec7d559f40f572f2bb74e":"":"":"":"2963b2932e86680bf
0eb6907777e88f6cb51c38b36794a0254e984431ec1295aaa26f91d5bbd3874c7733466e04fa4180fdb922b10604280a
1e34ba50b4f5867a9fd069028303364566ffa6f7410ae2194ee51bc951b19d7be1cce358e002a4b94085ca34f845bc759
8ed5036c23a1a1097809c7421fe0b6bd10e90d1f8ffd1cdcfaf3755bdfdde695b032173861ff3baef7a194b5e46c3b0a38
88f4e4696ee5dd2414a10c16eb372f67a7538782d61be0f7574646c7c05f6f3d81eae13b2f5327b8ab94d2c2172ea168a
0f2c6b79494b497da375606c7d04bc2d8d41618d925140b835b90ee224ffce041697af669b0a944d342524fb133e193a
54f4b528fbb"

HMAC_DRBG

NIST CAVS 14.3 PR False (SHA-512, 256, 0) #6
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"20f4687b717a31f5e818c872952385cd9ac2137abd2e49b9849f01cc2551dcd7f53dddb2449c1a9e793fb8a0447b303dd6da6110768f5d32766e3e3f171305fc68c4948dc6762d3c4d27c66fdf962cef":"0516d63709deee72cc6751191ea05d6aae7ef016dee1ad62159af167a785b353":"":"":"":"82ef3110200f4f322764f91fe5b119492b8627ece211e79e2ed69044e612f60553e5e50abdb1a1144e4a7afe05276c80b7d1e3992b609c4966f61beb02ff8ec889ff94889b69e4e6544be9ec760b260ede7e4b5e96b333fc460392efb1833a6467b175aa7d6602abe175ba16d94151fefa0fd1396960aa8c72a6b778f3f0674c86cbedff250b5a609d30e0b40ebeab2a524ceee7aa861b274bc55541dcbce77361acb8dd39fdfcaa02820950932245bd37986d5c1407098e13b5793666d079969b054589e70712d50be04bba484cb651c07971be722e13b82600358dec86c7f04c0c4e256ba12542f80ae7de745f50bfb07aa28e3857bcb1f371f01d93b12a2a"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-512, 256, 0) #7
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"ef41067a7ca9b6946155247ce8dbb619795f028d678ccf8f5f5b40e33e8cd15634db8c9141bc2cb0590a545ccd02cef6e1e96fea14fb8a55411d9ebf03633dae0ad449a2121d1c78fbc0e9cd8a78a34b":"7b90a2baa4c139e29c48db6c5b51ccf088fda54e4187611dab44409ce1c36f4b":"":"":"":"2a13126e8947278cfce11cb02ec31acccee5319d478a4937e8fb5e6483f5874fb20a17e9d4599d256b4d87318fff393f999e7f3d8612fc1b6063175a5d070805d53f7506632f03d37aa43b4e77e323ac0d5c241d9581d7e110fad21dec83d1dc9d119d1a0686636acd0846f58b42bc12a4e7e9d5ddbdc051515e8636fd3470a3b4c2efaf9774d78f3d32991f9ca50585f939d21a15c5cae6defb1702f9b606ebfd7308e55e6690310e35dadc48f9aa873f142397f36de90fcfc1dd0b8747496548b4688899df4d9d13857274741290a39c86d5b92d375b79efceb7f6cf2ac0c8c41e6d3c05f7e980628f330b5aad1328fb4b0621278b190758fafc93da359a3b"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 256, 0) #8
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"4d1a72a7a7efab609c6ea16e4a1150a8c1f8bcf19ec3225ad2eb10c761268d6d2c9b09f982710768aaff9d5e3337b028596f31842fd23e75a668063bdb03cf1d7e1ff419252d44335712f16720aff52b":"e5c9712ec583b2dbbfe76d5eea90b9e3b6815c2e38782192983c6a02efd91afa":"":"":"":"f4d994662acb2644e389b41c71122053b2a9bc68303f4c77870e426ac38c1b20d12cbd8adaffb611e3a3365defad82cc8c2a27d40f57e8035e16476442ce4c4beee9d8212d230f796fd92b02d7975790120bbf7a6af8115c06457d767c5543a6c1742ff745999f8e815f5caefc92b9540a6fd19ae973c52b321e7d4d7d9b6ab4900d13b7f633a7b8f1abe3e1a0540b5803b89d71b3c4d3a5dc7c4c0751e088f27b748440df9df14fe25096fdcafa1c3e16d49235defba82ed6ddd1fc8a5fe9f5d360bd72e0d19b21cbece29737037832b9ef18b96580ba50c344695d93d07b105f39c17cd91ebc291618c8862cd47459946f735fa7fc778b4489b574d6e77ee0"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 256, 0) #9
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"5c9f5de1e3bbb5193bbdabc6211e797dd89eac092995a5539ede5ee3f769c4c3e221e65efd6daebaf2b68e4353c23d08bbfe26b69abd8dbda8e41f4f9057ad7148541cca28ab0c3ea512aadcc65eef28":"17f703c54499fe53e688c6d48b4a0604ed9f6c71b1cb4fb9cde37eb8fd2a2ee0":"":"":"":"11c40f20930a9ae087d5ae4cd93c6d8defc073888f4f8e153b163e7ded25a3313a55b341d40315d78527ae87c932c9071ad6416823d266fe23000e1e33463d2f67c73c6883aa301e5f12820640ffb50b680c3aded1f6b93d21c3c1a9ea01ecc9642f1e653551d6e8fa8af6a8ef626def69c65571f4a26a7d8b7bad126d945961797c8147c3ecad4637f915f8a3a73b3ff235aa3c71273f0cc0e023fa26b8a567db56a456d58536807817d5f9b04fbbb99dca16164652526b4e84781f08f1501364a1e3b709894f010693523facd0ec9c61c41ad9847a9ae47f3b5ee57cdd63aa179caf1cc4957b59461aff01f08180a53334ed436697688c55608a12f

ddf7239"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 256, 0) #10
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"c5de35ca4848615697693d839616a4272900db5c894bb13fa3a43afb9e2a714c47a61871bed42c6c2a9d190b946f7201b671991c43e5da4325666b140bf96f0548a7220edf2dbd9bf0bde719061c11e6":"0678789f954ea314dabfce48d090bf93acaa2f89f7e1a92e6ee0f7afb19788fd":"":"":"":"7d4f29fe94ba8748d534f3fbfdd6dd8ca00f362eed4a84b2ea4c0ea83267246343271bc9d48d6e5c0265da7c11ea0a40ba8cef9ea76c649426d9089f0fd81b69a328ec511cf96e7ca79e7cf51b9fce4a62a8fdc568a4ff19604541ba2ea428eb28ae49645dc0451708fd53ee7e6e6cb8ef7607777f959a1efdc172c10e290f2f7f3b2cee2ce5e9a83c3928c55cee180bfa18359dfd9cfad1377cc0fed321ec9d13e4babc23e4efc89754648e9c6ebe7d7f69acda85a56501b8aa8887f9b809b29c7d3b02a8afc8c1ea9bdf26179b4547b480100c9e6f7d05edd620599d3ba85c96549a20dec8084dae4c98dca554a2cff094afed966a1b3109dbbd8ac5c52304"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 256, 0) #11
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"cf72dc871545003348cb2e458c6f4fd6df5220ce389a792f854498cabff1b5c88e3732f6aa95eaca2b318a4d29d2d33f3a289ceb1bd858e3c86c7404825c0c0a812064a05325e09d34553a691a601866":"d8df317e505af016e86297f02fba94059b4cd31529d8c1ee1b33107df753d89d":"":"":"":"181851eb38a67d9552c87902d25c67afd377aee587da12386a46148c4cab44ed5b61777c2247d0d39e0991fa6462475da9763d30f1adc9a1d2f90ee3733cf335648706bc7ba06c862ec9969a0ae38b7b1e14817e0d1dd06bba77a7371f60e0867fd7744b0b4b7e36cc1e280236fcb5193c73a2d00cd0c256b44eb6497ecd69d1669ad3eec8a4e4c8b730d85e12d1d9c40070e645020d7ae2360cd0d39d559713b4f010a318dfa91e44549fd85e5ae87bff1547305be5b788b5750ebaf11a60b0ce6d26dd69d219aef1a9a038ddaee0e8135a4428062837af5e0aa1be821af0246c6076ba9ada4e0aa7f74202e10802879142cd109cd27a292d04e6c53e33db0d"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 256, 0) #12
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"c89dc15467ae09d5c514a0941f3945b1f4a1670a4df9910d14c68aa6d3c36e8f5bae0abaefd8fe5300b56a7bc38083b55602025c221e1f0d1671f2ae92bb0c86fde571ccfe8b8b5be8a94f3f1d027ee2":"8109ddb29d8395e938aa210852da6bf1f1a3d00be9df74b372e081d538983174":"":"":"":"e1c5d2b4ef29b2bfa498541be087f21075b0b7449ac7fd234d8e6af45680920bbe1dae35850cf27469209162d4175ec42c3d5cd6b7965f95948d9c49eea2db9dca83d1bd8bb49093ea0af12497bddd8cada20bdc94a453792800cc66d01cdf5e0afdfbdef3cead291e5b88b116fb47b82b4b18d6fb363d733718496ea20ca2614caed61d823ca9923fcd2f570a9c03827187b0cfed19bcd2c2e87f58508da8e1096eb9eb4c2ba223cded5064a6a9b5eed8cef6fabe3aaacb88b58fab570a56e80cade1be8c82f3b6918a7e574c91dc4fddac497f1cf26a801d6cf24ce49ed5e8bafbee09eceb39e1f81821ef5477fa0394992c848fd2cedd8f86c4c4a396eb3e"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 256, 0) #13
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"1a100ec0da9544326286b38705523ac970b896ef6e6306b2124e283a8851e46d3a4b2bc6a8152ec9b0f88d0e2bd1528b13ea307a3384c10d1fead60b90bf25c305a91558c1537e2a7ac74a85240208f4":"005612d87b6df0204c3d879b5ca30bfc49df4e189285307e2926b367ebac30ff":"":"":"":"01f56c3a325a39a2bc85e6e077b7a2864921a4b223c7fe998ae255d724a759a66971084047b44fc1b8ad013e976ab8b255930337eda8761

2364d605f241095200f8a8513a612bd847aea116b73078349b7cf60cd2588a8f7431671c3b3c6ab2e4dba9796b1ddeb2e1edd4cb3c4dd67cf722679cf64c5b20c64e28be1ac87f8cd9f17b59ed696f61a4a472fdf37aa90a2f16edd3d54c5abe7dcb0e964bbfbc113e66b1887e0daa2151635b803c0340ba55e3e5817cde2662ad45133c277502400b78272786c7aa40c54219a06b5a32e088baf0613fc535dbef66241befa09722f3730bc85c0434c733ab17dcc7c473d8b9f31651921407d85369b6f6fb609d53f"

HMAC_DRBG NIST
CAVS 14.3 PR False (SHA-512, 256, 0) #14
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"47c42df62b4dd570efd3c2722ad39a2df5f969a13f645fd27b5290877ba70916c591934d4f66000ebf8c508fafc44f75d16a2c72c63580b9bcf156862214533a47b1686c871a0165604fdd00a412a484":"94822903cb5c2003c31c6d072ab0dda435add0de7d8f9d5f08b5cba410d888fd":"":"":"":"f78e61b443b5a97b7e493a8ce35a43545290dd33d15ba4bf0ff78f34a25c46c4ff4cd485964cc96e90fe847d9fc9e42d96e4f5aaccf976a84e3e12100c28b0f7addb1c76f89663e11890f09e4beefe928a1e0b304f1d9dd0414cd115a01b641fd69c7071f2ca7c7f2e53560f4e91010ba11948195bc5deb556686feb0bb92fe61b3171e639ef47418f02be37796efdb6920952f3a8c766b52fccfa757e923e38028a84f9be1b802c1fbbbb4aef825f4c5e4fc1bf6e96f33ab90ea486710718c9e4f3247b2a55ccef5a5d342cac757f0b9f90bcdcc8c2ec3a43149bbd3924c85f0b5b7ae42151f4ded826ee6d47849ef4e8af64adf6863982503c23c4a0514ce0"

HMAC_DRBG NIST CAVS 14.3 PR False (SHA-512, 256, 256) #0
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"da740cbc36057a8e282ae717fe7dfbb245e9e5d49908a0119c5dbcf0a1f2d5ab46561ff612217ba3ff91baa06d4b54401d61d4d8a41c3254b92104fd555adae0569d1835bb52657ec7fbba0fe03579c5":"fc227293523ecb5b1e28c87863626627d958acc558a672b148ce19e2abd2dde4":"b9ed8e35ad018a375b61189c8d365b00507cb1b4510d21cac212356b5bbaa8b2":"b7998998eaf9e5d34e64ff7f03de765b31f407899d20535573e670c1b402c26a":"2089d49d63e0c4df58879d0cb1ba998e5b3d1a7786b785e7cf13ca5ea5e33cfd":"5b70f3e4da95264233efbab155b828d4e231b67cc92757feca407cc9615a660871cb07ad1a2e9a99412feda8ee34dc9c57fa08d3f8225b30d29887d20907d12330fffd14d1697ba0756d37491b0a8814106e46c8677d49d9157109c402ad0c247a2f50cd5d99e538c850b906937a05dbb8888d984bc77f6ca00b0e3bc97b16d6d25814a54aa12143afddd8b2263690565d545f4137e593bb3ca88a37b0aadf79726b95c61906257e6dc47acd5b6b7e4b534243b13c16ad5a0a1163c0099fce43f428cd27c3e6463cf5e9a9621f4b3d0b3d4654316f4707675df39278d5783823049477dcce8c57fdbd576711c91301e9bd6bb0d3e72dc46d480ed8f61fd63811"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 256, 256) #1
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"c2ff911b4c93846d07e0d00eeead3423845c7215c8b5fe315aa638745e63ca26f1062321318087bf045903cd4f5cc9e61a318c2861c6a93948d779ab45f14d451bcef2d43a5ac752995bc0b365bc3fbc":"b62f8ed28a72c28d80b41e016f559bbda0a2a447f8e146eb93a509b302e03c42":"77aa1ff77bf037ae26e60d412f3341715afcc1fcd3bf971a481a15d45c794331":"55ca83dff075f4de57588dcec9bcf0fd1fa267bc280d3c48f1f1f749e1997cc2":"e42e4aeca6716181c71ebd462082309868f6faafb5d9c82357c785283f6d5285":"384383c41b4df205d19fe68e563dbfcd2f6edbd176574248f3d1ee44143b70aa5dea695b87bb6c82378953a714084ebb5619aca7d63e0dfbffc253a336edf80acbd584cd3f916d6126968d564c1dabf7b3479a62e7dfce560b80a5104389bcd771e20138dad4c59f290a4525b00f6798fb2a3c8f44605a247653d24c772d207f0ccdc19a07037429c7e79771c6a6b4ca219a1f8ed9bbad9c4cb27415d18b7278552e50ec6e25617cefa7324ad786aaeca811c3aaa35ae00d2f2152fb6d98dca82ebe579bedbb50a40e62af9e229dbf9b9b2bc6532b5d78e6333cfeb1ad01e192491193c9459b78d4e9c6e8efe69cf0c702298e325f129027145af92170b843a5"

HMAC_DRBG
NIST
CAVS 14.3 PR False (SHA-512, 256, 256) #2
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"e1a333ffe4bce7b9f6bbc8dad8787a82ad66ca9b25a64f04b166face945c249b5f45cdd318c0588c7cbcd14846523943a59119683628020e901a0a7fefc21625864ecb1d76ec119a10821b49a3431348":"ce1466063de221c4fa1cc308442db476acfd8ff34b2a0dbbbe0eceeaff210293":"d481e022a80f3e60687bf153524a33bd6fe42c54c39a377a9fc27e047df53f14":"26a88acf67d5ed00184baad664c6b2d4a91d437a121c3cad9eabf3d7e676b0d0":"524e4896a22bedc62820c500ed7da2bbbb4c1ef9f07b5f374d0fb4ae9bbe50e1":"3c3cfdebca060f534a952e4933c2c00f9ee0fcb825a58abb6aebc952e160668f711068881ba8a6817500bba1c28867cf21a12a50e46792abeb9f41bc02322bce1e77d236b7a45a7807fe22b8ea9e2859d2b0164783d364f6ad84f4b9341c576cd6ab2ab249246bd76910e0abf115e4c59e37074de5f4defd03fa61ce1733e33c98849ec28ca61b845035218afa7ee2867b32ba1efc50907d76ccca5a7ba69e9700875b200cec5d1fadaac77a0960c4eb899c06134cd9cb663c62b69446a460bc9e3df7eaf2a34df00fcd838e882f5af1aa701d35dacec0cafbe74cf6dde7893b880071d3f1c9e53b205bdfde9807999e73468264d6172c952a7f5f88a836b1c3"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 256, 256) #3
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"73cc8caea7f1f2129bd035b77bba2309ca3bec73e9f993fbcce7e3f148670bca656e3f17e5a8ce9bfe3665f4b6ca8ac8111fe051ee0e760b295b73470da27081ff17bfcd6ff9085c5e064ab844927f84":"eef338ebdf4d9399441655090136becbcaf277e5ac73426f79552b3f27819ab6":"2114d320b65a5906d04c5166ee82e727cc53f0ba33ed54a3229ad9592995695d":"e3fce46cd5c90936f20252e0065dee1940c7902198ae105017a8f50d143a50f6":"7ad27ea94de6ec7ad7cc1895381c735f007f6087d688a070b4cdfaecdd2a3345":"858108fe1adf90fb3238363ce3532362675a462563e5c12df97d054267df0b205ed3960d86893c93d2b1997d95abd9179512289297b00cacd1a51202923c4224561e9986d0242f50ea4667fd6402e29d18c184028cc6c85836b1455e2d2e9b389e0d65bcd2c78d5e42ad9e47707c9dd4617e6ef2d64590d0e0be5e4465eb611d91b1a45bca1af04632fc8dd045a5f5ba3ec1fc09e3aaa1d03719181e11c80dcd1c4d1aac3ca69d89b9d2c6ff7575d78843fc4695c1954fc663732418bddba4b20439da03d0428fa047f99a378447f9e563fe405fd8f9c32d580aa6dc1560b9df1530fcc7b337072cb60007b4e2762dc61a08e6511e7c93b91303aa3d46c14483"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 256, 256) #4
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"5eedd039764e7af96c3ef7d9e094e861dc0839c2a2642c4082afd09f2761c392a4eb8fb607ca7c5d7d4eb8e871aa995037a297af07ba36a59572e3975138fcfea667e06d9a4bfd2e9c570e61fbc09006":"92a258c0ca5a9c030dd469ca5d8883ae5f3fdaf7d8e0fb23867d150f3d24a0a9":"954a9431a4f9b34f6c28fc41be05fefa3449c8ce0265a19b8a422935690b50c7":"1765c701b279cde38b469bf0948f500b5afea8f7eaac3f100ae5f0b147005ea2":"1f6d382b8a8967efb9feffb8557f1cf40f4f65b5fa7d9846cab0601f5150430b":"bba8f496d47ec97d90533650275243fe76844b606d714c8bdf37db1e3f8045de44482d65a99b6d60ee4aecdaf0d262d96c058dbd704ee96e4ae52bd3ea56e9062b93e2b044124b7e9304dfa237e623d7e7bcedf59bfffee1c581c7e41a401832443ae80c6f4b7643591bd78254996235d011233b18d993b950ccf09bf29b2ae10b85e4cc4feba5503f8e81b0d0e7b50e7eb1a358726369e4af07ef64aa83813e61350068026161a3ccba808a99d11e7de5afdd91137fec9b77de8b59ded6286e590ffab21fde191362af132bac1e8170f36f95d53593e73d1775609a0ef04d9a75a4bab26f97d253b8e00ca430841cb5bba4439124abd37fb43f3510bd5690bc"

HMAC_DRBG

NIST CAVS 14.3 PR False (SHA-512, 256, 256) #5
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"95e33e3e1e5d24dcfbc5a534ad0e6ab6ab15dd6b094b7642e2187aba9a303137b5b7dc3d70253c3a8b446b591fab6950c4f6a33de5257fdc474a46ebbd367465127e6a9eaa97e17851f9a4d55fe4e954":"7080c7d4ddd8e32fda42ea23adddf7a4d3893be2cb87d6c7293bff521c252189":"611ec30b87ddd1096396d539ec973dcb7c408a62e6c37bfbe563dbb60d9f4932":"8a4a0f9eee67c54e3dfd846ea92981cd769a8c7ff4f2646c85e80a03fc556bc3":"05dc36b5d354f4c3b950053f925616c27e2317f886d2af09ec1eb7ac5397977a":"90fe978fec5cb14ad180e1ca8d3e266658efd9b0fc95353d4edd06c4682572a46e918d1bf4269d38f5b005691f4b5a8ded08983d307a0d7de64e681a302ea6d0ff8ddb87bcb5ab0871779b10744d8188f7bf2d6498a4ee998da93d1a2fdf3d3da635c52cc26977b25dfe17a5f5dcc80fd72d066db7cdbeda557ba52554e1ef5a075d7a40ceca83cd83477d99591228f4ae33163d73045d35bdf892cd21083b8d70a3297212edeea57ebfb66baf7af38833e72113001c2489ea4beae57995169a1354131a7f607a1551643d27f56ce8e96143a78b2a19f9fd72cae9054533fdf16825d852c990dbcf347d32529952445cacc55c79a79c55ebdda76f226bab80d6"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 256, 256) #6
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"b43301c1af024ba6cd7eadf985cb1c6c303479ec3ab47797392d4220788f4daec2b1f5ac6138bcb83e938be66b3232f7f022f4e548b93e7a8aa4d853fc1b4c42ed9b182ae582f6876beb268ba23c4105":"ad7fcba1f90b243689b85a4ea1dc150bbeca4093dd8b9a0a491a678011ad807d":"0410527589e72024491d4b5328b5659a330d9b167a1a27251363e262f393eb57":"5de8fac62063a676904aa9628046fe71f080ce285ef964acdcd11260734f2d90":"2f14a327bdbb9be4d9a813dd73445c8a8c911a874daf08a551e867f54983de2f":"41d553adcd069c7d2b265798f8891329b1dbcabe2e7c03502542b322d13ea71cd8272eeec65d31520782351a33915deccfb8e10cb64d5f9cd88eb30608f7b136486b5972a68b981e0b9b7298bb670ace568b98c88d35b4a40c25bedec94eff992c0083e539adccc37ca5a4093ac96aa13c83a59c080bbe02e37a81303500224daa4f380d2b88cb84ebaac342bfe5789658585d2892cef2bc9ab6f1ad51fb292e531bc33186e39b93fb67d4ac633a2f4f8c681c7f82a81a47b74905613bf10ebd3c57fd6c8624bc7e55b38e2ad063aea90faa038d671f86c6b17d4341032e11e13c526c4818dfc42cda496ecc060d9a1ac45ae0e72a6e05bc3a8aa851af5214b3"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 256, 256) #7
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"837e9048e5564df02e25f7b7585ac5600ce4cd6a6de8311c6b3c6084356ad0f9fcddad47e7bb6ad7ac9f33145de135605866611c2b083fd1f9e5cea98f2725cdcfb0d2ff6f0adb74d6fb61f8a6ca02b0":"1d194d69897c5a7e8c36cc4cd97784312c9b6599274e3b20d022b1349ac45c58":"b6a8880d415cc4b2aadaad6d7d2dc73484b70909345bd209520c05fe7f5cdc80":"31bd3fc264c252bd3f8102529763d5ad3e45a4e068677423e698160db284bf11":"0b845cf842d1ccc15c2fa7224ad121b9b5f8acd1e07b16c143c931da56620906":"7a6dab28ae7231e2dbbd826c4eedd8ce062df31fffbb0c0ec045b0cd0a4e3457ff978bf39425e48cbea4884fc59e95665068361a8ee9175a48ef094806fc146ccfc3c403a770abd0c6bc8439bf68a89f13b0725a79dbaf976dba95725a4399c58d15c4758a515346cd0d6208fb0bccc06568642eb3e0c3a9a1df9567eeaa86924157ccfe5b2f8e8ec946871dad33f40f65847088c9e500faf8e25439be8a1e77df12a2b21b9f73244b82176e4bea4ed33d2671eacfa5c4b591cd0bd93dab7dc62f7231840909ca319278185f873d00820fbc239c3092d1dc1a3cd9c692ed6d37192bc587f8b3ee21c14fb20c520fa7899bcd2a1a53288a42cf70c6fefe7ef7b9"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 256, 256) #8
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"f840c75ce0cdb200a3bd980d6cedf1c7321e5f303cd0446c7afd2d2d666

57447b215333b15d55326bc9bebae6ae36efea3a337c6fbeb6a979a4783f2b7f0f0dd6d3a9d3747de639a9047248a04a19f5b":"6d5ca4b1edf6c0afbdce02ecb30923b2f4f2b33121e21b2ffee964cc7de1abe8":"f56d2b1584ba2f129c77b29590c4e1dfdab5527b1791e3e445750ca6d4ae3542":"05bd799249411b37b80590d49f3348631b06a2408a61635c70687003a8485302":"12d26ac3b87924cda5d78a3e3c0bd81280e340723643ed1b2ebf2dfd52f5dc43":"b48c13af7a9b6fa6385a7ee5d2ab97dcebf71a715dc465f413cb0962292df84c9c83c4093309f749359b0a0ddcc13162cb4ab8ff7b3a6336351ed79ebf47730f97accb6a960a9c5c25e0920a06cccc3b3f62b616c15ca18d7e0b5c2e7d8ad2518d1ef0bef515af866893e9378b56deec32825fe0a2c5a9729f658915b99ab22a03b7187e83d2d0f41b9467c8326f7bc87189dd8ade18b3a7edf0c0ea462dc22109ec91294cf8ce69c8cd0c129b423edadda8fbd25f4983a70d75001576a26405188bb0284975203694c318f3aa7fe47ec041bc4c11c9bceb1b131f74adcd72fc4d2813564de6d4711017800377be9e4c579e88464d67ea6e457a30f8f652375a"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 256, 256) #9
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"c91db86e3984dbaa25ae5d851ef341eb647bd1df0517e171fb86069cf6183c19a386746ccd0a7e81f3557038711db7259926089317ab7142d6ab6050b1f7dfc21080910d43a702cce93cb1d3b155d22e":"a4585c13c83f962df72b58230ea123846df652b2810766bb671f675b96125a4d":"fb31319b4e622dedaa88b64aed93bb108362234c3d3ecefc78f796aeadd9c8e8":"877bafbab3bf9c20b1a85a5f4b3dd11a5c486042b807c39d59fde1eaed89cced":"89a5af332718418758129b8212643750542bf957bf35c64d6b0a276238c808f3":"931e43b1607f43260ca4fec3205bafd90ccf9916d721d9edc384250f9346525c7656cc7b5aed8acf92b8d843108855ac13f4f0903e51aa4ab7846a839ce70b7de88e0d52590ede14437b5493b6c2d9458d221b771107ec166f66ed993739604c487fb4ce94bd795e9cff60b4f8365c758c27fd767135b90b3372570a8e0e3b3a23da37e69382afbb76168ace3ca78852bf99a0d3a7e2bf192d8d929dff5b07730e00a8c5fa5ae243c89e71fd52907eec0b4c49fb86b81394e38a6b0523a89c0fc866c2c3cf76f336e9438d4f773cd5ceea4dd47b3716a9986153f718177d2c8ebcfcb90b986330f817334d29aeb9c93e9da5db30b483f8f434f2807bddec6851"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 256, 256) #10
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"3e4c40b9b33063edbfd21bc4e34c5bc1f454d7ed176e4f6edc3ab056a3b0d1a79170479fd91d6e30caf99166842e0175b2941a7186d8c3f54e6f5f9884e47dd22a161a3fc5e00c1c9ca5a744c6a7f7b2":"7a3d7511b93842159162176b7016106e61573aa42c57aca7bbfc97b3388c28b3":"d88781b3afe2e1500b6881aa9cc23dd150054da57be0ca127e101a9fbc4decce":"6231b0f5cf182c6f108491c5b7ebed9b2a015e9698e860623e9a12e691a38899":"bda666c5ac006d6efc2aa0da52e74eded88955f8f064bfaa52d9f2524a195f59":"2d7d62310bfc4a3347122e23655a10dfc54fac51349f0c8d586aad39236a20368f4d96623e58987f7c1184148d586022a4b96976f72636eb1aa92ad221c5866b6c6803cbf6c982e1de12bc89618aeb3f844b2a518a578714e2380075acb828685a57683179753fd1ebd2d8aa1672940446756829d6ac1cafbb21858465789adc024b8fa544bea09cd4f1f3ed35f298d4619a5f92a6e4f712a0032307ed781166d7a6af2a352694be7fd3bc8a151ea848f8b14da8150eb22e264d76e655fdb3638bf250546eb29ff27850d2b5697932c6a876743561e0894a01ce8435cef74800f11e4bf44fa5149a6fa4f4ca43267a47d3841722ae7efd09676f341a54ff1bc7"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 256, 256) #11
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"fe4f5247dc405c12133e9cf7fe00483649d0e7b70fdb1b39f8e8ed0a4789a0c9ab78417816b54d47cf98c0aa4246ab0d68028d1e7441ab77c5eaaf9aba0f2ac6e1be2af480026d44d5eec0e46fdd31b1":"5c5a5e517b3acb6d6d75742bc293e4d091d7b0bf37559f75df98d6306bcc2d22":"5f56dc4800297a3fa8e2b38483c29505485628866ff175b19d4abaf4526bad92":"d9bc081026ea5e35a52b9d1868688e03aed785af201e355cf51e6e8c

ec917c34":"bcec655ee8c482e725c5b915b4085a9d678ea26b71c1ce0a85f741f9fb3c3607":"411edcadb791507f40bfd00f3c764a2c758729f3bea116ba0c820efe09ed379095f7877cdd6c694c436572f4dd1b905301ed6e5fa1360ac8112860307958c7b64372eae8f4122d84ff2d4b690419e3043b8a6183afde8f084fa110c38403adbc878b9b139f6df5cf47adbec2d1f03cbcfeccc412942346fc42f0af77d52cf9127dfb02beae47375aac101baac38d0b47d8f04f83a7eff482ead937238275308693906303797 67df1f40b73932789583da327e2f363ba421a253d35d205b00945d9f5521580350f631cb24c7bcdf7cdda7cf28baf625fd9d61134ec7a6d1cf4c80d05441722d081d4aea1074712f37884fe15ddb3cebdadb20e71cf3ab41676fe"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 256, 256) #12
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"9d129142ba466c27f348d5949fafb79675e334fc3a1948e5d008ee265076467bfa435596b661c527a82e5a064fd56cb6f17f549c77a0a6a998712ef0e1f41ba4eeb354f77565f7a7627eaeab83ea48fe":"ac23c42315f2bbe54eba535a7299113cfc88216727ede9f154d7bddd88041259":"7f029d2430d49de4909a758a2bda4f219d37eff01c96de7ca2a4071d128a1c9d":"4b6a443312f10348f6aba088d1f81206c696508a75836e98951604e93fa6db51":"bc128051ddc96eef9fbc3a23ff458240d11a229d1a75888d622ceb7519e1db6a":"03bbf9e2c0c1abc1ad71506fe91d483481fc583a73ed2eb4c8834a87118088b20474b78e06366b2f32a5f50e6425be841e1885a72aa106d5a001e3909b1ac2a29940ded83f0724514800aa0dbbb18da6d573aa97c7de470e115e9332179cf8b321fdc83265b4d58ed39c28d09783590704ab9adf007ee44d4d74af437851734d470085d45252588d75448abc608be03630152582e0344e1a7522a87c3daebeefbc79497757835f079dd99260ed7d7e3e00bdf046f4dab3ca84b203f8c93cde99755c2f5b16c00d00f370715f188e80f3f353f2d218350fe1a9f68673ea8e9301333fe5ca7c703d21aa2d0df020db28d8340b5e2c07ce5bfbcde7194399b6f752"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 256, 256) #13
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"2fba8ed5b2be9af95fb02183ca8ae0dcca90b209be73511a5dab31ec81e939117e529fca4f95a483bd307838ef0d779dbbfe77df481d807b309da929f319b39287d3ae0994f77ff616f0a763f35d44a3":"2de698d32010618c25ed86cccad2ea4d9fb9adf7b3dc400a2b1b4c975651d103":"f9ffcfd5bc9a08f6f9059f4bb7f49e093f404aa7fe736bbf4018734071c26334":"a309fb1f43a520a22946a6418500929e19d2b3316fb1a8c1aa5d047ddfdb8d49":"c1dbfdb9bdd4a3321074b57e11e5ec6dfc374248a918242fb3e22cc6612b3239":"3eee1bdb63433c55971297e15ac1691cbdfed576b1d2ada27cab33e660a3c8575fe989ef73e13058c9a3777c35bff1dab25e1991b78cc446738ccce723eb02136fcb24a0dd2597c3fd0a75774c4a21409689e9309e962be1e8b096c2dde59ad9dc6750051058ff6a18d57a19ec2775882ea0af65b172ed718678d841fb51437aa3133b2b328df0f4ac916a01d88c740981bf71c4664789ca4e9d3f7fdbe7379231b64683fc891c5222f8b396a446f3b50dde823f95177b7284663402fe5452fe7bdee304abe34d71172170ff3a911782b72b2556f2337d1d23d9d632bf6831d3c173fea3ca8eb5d7993a58a4b9f8f64d5c89319acbc847576b383fae0178a097"

HMAC_DRBG
NIST CAVS 14.3 PR False (SHA-512, 256, 256) #14
depends_on:MBEDTLS_SHA512_C
hmac_drbg_nopr:MBEDTLS_MD_SHA512:"a9fd18764900768b7909db87dd4c7b87baa2cae6b0f62a8c2ee3e4c550041ca7435c7b35ecc6ef373dde3d989420b92c2bb32f9fc8c766ab840f5d0c73558dcac87e2102c28193e7ffd3381bc30e1d31":"8bfc5a65fa21396081d92c3d7206f92637389c60cd7a14f11811c91535c0083e":"404236bfe24b471ac7df938be6a96b8ebf8bc758787714d226ce727e9d2b4bd6":"8151ae3237ca06ca5b0373039681a9d3cf799e98c3fa2efb576822f1fe0aaa06":"11f0f8a2c16b1bc15fc93ff4793894f22d7494d11c94dde5ead2f0fb09bae6cb":"9c636c3228432fb70d521eaed3ba8e436507e29163de0f5b7e0aa9a5177aa1a3930b95f72fb0561353db7213cde9ebdbd9485a5df93ff416966e09c1e61d8f805e6a082d6372d58301660a9a0181e2ef906a5a8a999c88002eb4b4132b34efd21618871ce28be5e66a65

a1782de11e8e11c57a2debc85b0068ab553400b26a0a0f948ccb4e8bbc1173dcdab388c20ef6e2c9ac796d8816572ebc1
34396d38d71ba8e986eeb063a7baf5ccdcf583a723ba56bec38d4cd3e7bea563b4132f19b730189f559300091e9171a61
469460ca82d39b5148e4d288037f6926e96f384eaaa0efdacf2ad93f0da4fdca0bc5ec0f0d7c0e8dadffae4e46ae96a6511
735a80e"
-----BEGIN EC PARAMETERS-----
BggqhkjOPQMBBw==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIJHLciDhJcnlE5MhTrOfFlnRbpJQLOf4h72E6VDXxMM0oAoGCCqGSM49
AwEHoUQDQgAExnm6zfCcRIXjnQsQ/poZ0OMzFMRdVlJJgAByFMNPPQWIh/UgMGEv
zObZ5fkfH2476BqkqUek5FfRFNwkMiKMcA==
-----END EC PRIVATE KEY-----
add_executable(hello hello.c)
target_link_libraries(hello mbedtls)

add_executable(generic_sum generic_sum.c)
target_link_libraries(generic_sum mbedtls)

install(TARGETS hello generic_sum
    DESTINATION "bin"
    PERMISSIONS OWNER_READ OWNER_WRITE OWNER_EXECUTE GROUP_READ
GROUP_EXECUTE WORLD_READ WORLD_EXECUTE)
-----BEGIN X509 CRL-----
MIICJDCCAQYCAQEwEwYJKoZIhvcNAQEKMAaiBAICAOowOzELMAkGA1UEBhMCTkwx
ETAPBgNVBAoTCFBvbGFyU1NMMRkwFwYDVQQDExBQb2xhclNTTCBUZXN0IENBFw0x
NDAxMjAxMzQ2MzVaFw0yNDAxMTgxMzQ2MzVaMCgwEgIBChcNMTMwOTI0MTYyODM4
WjASAgEWFw0xNDAxMjAxMzQzMDVaoGcwZTBjBgNVHSMEXDBagBS0WuSls97SUva5
1aaVD+s+vMf9/6E/pD0wOzELMAkGA1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NM
MRkwFwYDVQQDExBQb2xhclNTTCBUZXN0IENBggEAMBMGCSqGSIb3DQEBCjAGogQC
AgDqA4IBAQB8ZBX0BEgRcx0lfk1ctELRu1AYoJ5BnsmQpq23Ca4YIP2yb2kTN1ZS
4fR4SgYcNctgo2JJiNiUkCu1ZnRUOJUy8UlEio0+aeumTNz6CbeJEDhr5NC3oiV0
MzvLn9rJVLPetOT9UrvvIy8iz5Pn1d8mu5rkt9BKQRq9NQx8riKnSIoTc91NLCMo
mkCCB55DVbazODSWK19e6yQ0JS454RglOsqRtLJ/EDbi6lCsLXotFt3GEGMrob1O
7Qck1Z59boaHxGYFEVnx90+4M3/qikVtwZdcBjLEmfuwYvszFw8J2y6Xwmg/HtUa
y6li0JzWNHtkKUlCv2+SESZbD3NU8GQZ
-----END X509 CRL-----
-----BEGIN CERTIFICATE REQUEST-----
MIICgTCCAWkCAQAwPDELMAkGA1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NMMRow
GAYDVQQDExFQb2xhclNTTCBTZXJ2ZXIgMTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAKkCHz1AatVVU4v9Nu6CZS4VYV6Jv7joRZDb7ogWUtPxQ1BHlhJZ
ZIdr/SvgRvlzvt3PkuGRW+1moG+JKXlFgNCDatVBQ3dfOXwJBEeCsFc5cO2j7BUZ
HqgzCEfBBUKp/UzDtN/dBh9NEFFAZ3MTD0D4bYElXwqxU8YwfhU5rPla7n+SnqYF
W+cTl4W1I5LZ1CQG1QkliXUH3aYajz8JGb6tZSxk65Wb3P5BXhem2mxbacwCuhQs
FiScStzN0PdSZ3PxLaAj/X70McotcMqJCwTbLqZPcG6ezr1YieJTWZ5uWpJl4og/
DJQZo93l6J2VE+0p26twEtxaymsXq1KCVLECAwEAAaAAMA0GCSqGSIb3DQEBCwUA
A4IBAQBY/1nnYQ3ThVyeZb1Z2wLYoHZ5rfeJCedyP7N/gjJZjhrMbwioUft2uHpb
+OZQfxRXJTbtj/1wpRMCoUMLWzapS7/xGx3IjoPtl42aM4M+xVYvbLjExL13kUAr
eE4JWcMIbTEPol2zSdX/LuB+m27jEp5VsvM2ty9qOw/T4iKwjFSe6pcYZ2spks19

3ltgjnaamwqKcN9zUA3IERTsWjr5exKYgfXm2OeeuSP0tHr7Dh+w/2XA9dGcLhrm
TA4P8QjIgSDlyzmhYYmsrioFPuCfdi1uzs8bxmbLXbiCGZ8TDMy5oLqLo1K+j2pF
ox+ATHKxQ/XpRQP+2OTb9sw1kM59
-----END CERTIFICATE REQUEST-----
label_1234567890=643808006803554439230129854961492699151386107534013432918073439524138264842370630061369715394739134090922937332590384720397133335969549256322620979036686633213903952966175107096769180017646161851573147596390153
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAyHTEzLn5tXnpRdkUYLB9u5Pyax6fM60Nj4o8VmXl3ETZzGaF
B9X4J7BKNdBjngpuG7fa8H6r7gwQk4ZJGDTzqCrSV/Uu1C93KYRhTYJQj6eVSHD1
bk2y1RPD0hrt5kPqQhTrdOrA7R/UV06p86jt0uDBMHEwMjDV0/YI0FZPRo7yX/k9
Z5GIMC5Cst99++UMd//sMcB4j7/Cf8qtbCHWjdmLao5v4Jv4EFbMs44TFeY0BGbH
7vk2DmqV9gmaBmf0ZXH4yqSxJeD+PIs1BGe64E92hfx//DZrtenNLQNiTrM9AM+v
dqBpVoNq0qjU51Bx5rU2BXcFbXvI5MT9TNUhXwIDAQABAoIBAGdNtfYDiap6bzst
yhCiI8m9TtrhZw4MisaEaN/ll3XSjaOG2dvV6xMZCMV+5TeXDHOAZnY18Yi18vzz
4Ut2TnNFzizCECYNaA2fST3WgInnxUkV3YXAyP6CNxJaCmv2aA0yFr2kFVSeaKGt
ymvljNp2NVkvm7Th8fBQBO7I7AXhz43k0mR7XmPgewe8ApZOG3hstkOaMvbWAvWA
zCZupdDjZYjOJqlA4eEA4H8/w7F83r5CugeBE8LgEREjLPiyejrU5H1fubEY+h0d
l5HZBJ68ybTXfQ5U9o/QKA3dd0toBEhhdRUDGzWtjvwkEQfqF1reGWj/tod/gCpf
DFi6X0ECgYEA4wOv/pjSC3ty6TuOvKX2rOUiBrLXXv2JSxZnMoMiWI5ipLQt+RYT
VPafL/m7Dn6MbwjayOkcZhBwk5CNz5A6Q4lJ64Mq/lqHznRCQQ2Mc1G8eyDF/fYL
Ze2pLvwP9VD5jTc2miDfw+MnvJhywRRLcemDFP8k4hQVtm8PMp3ZmNECgYEA4gz7
wzObR4gn8ibe617uQPZjWzUj9dUHYd+in1gwBCIrtNnaRn9I9U/Q6tegRYpii4ys
c176NmU+umy6XmuSKV5qD9bSpZWG2nLFnslrN15Lm3fhZxoeMNhBaEDTnLT26yoi
33gp0mSSWy94ZEqipms+ULF6sY1ZtFW6tpGFoy8CgYAQHhnnvJflIs2ky4q10B60
ZcxFp3rtDpkp0JxhFLhiizFrujMtZSjYNm5U7KkgPVHhLELEUvCmOnKTt4ap/vZ0
BxJNe1GZH3pW6SAvGDQpl9sG7uu/vTFP+lCxukmzxB0DrrDcvorEkKMom7ZCCRvW
KZsZ6YeH2Z81BauRj218kQKBgQCUV/DgKP2985xDTT79N08jUo3hTP5MVYCCuj/+
UeEw1TvZcx3LJby7P6Xad6a1/BqveaGyFKIfEFIaBUBItk801sDDpDaYc4gL00Xc
7lFuBHOZkxJYlss5QrGpuOEl9ZwUt5IrFLBdYaKqNHzNVC1pCPfb/JyH6Dr2HUxq
gxUwAQKBgQCcU6G2L8AG9d9c0UpOyL1tMvFe5Ttw0KjlQVdsh1MP6yigYo9DYuwu
bHFVW2r0dBTqegP2/KTOxKzaHfC1qf0RGDsUoJCNJrd1cwoCLG8P2EF4w3OBrKqv
8u4ytY0F+Vlanj5lm3TaoHSVF1+NWPyOTiwevIECGKwSxvlki4fDAA==
-----END
RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDcwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDgwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAARpQeQ/YGQj
nl7Szo6WStJ1u7xunTL5jBkXH8aAVSm0qiX4AD/7YPxa5EnGzZdLTn25vQVnfQAG
pMx8P1lYiGYCo4GJMIGGMB0GA1UdDgQWBBS40mLt93U8Sh8ZGiDVAhRSiBPcXjBX
BgNVHSMEUDBOgBREq5J3toJPxZ3O+ssJ5vkkU0RJE6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA2ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhANwGf+F4a+kmXWz8UjSpRkaToTV6EFWw
/Tjzj0tQhDoAAiEA19RxeWOVBBpM6LOHg6v5Lf54YN1snkLf+sEXyZCuWQQ=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----

MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDYwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDcwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASNOj4d4MEA
7p/3miijqG4ToE4opKPAm+3BTIGrJTYT14++TSiUICl0ASXj+xeUcLMIaXTN042s
LsHxpShzQaL0o4GJMIGGMB0GA1UdDgQWBBREq5J3toJPxZ3O+ssJ5vkkU0RJEzBX
BgNVHSMEUDBOgBSjovYaC/m6Li9Tp0V9iZRs9267Q6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA1ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAKGcf+c442c/XiwubbaiQvsoZ7EoVxuM
oKmia0gPyBNkAiEA83asjJ5FDXQuLyZpczviXrbmqgCPOfYadtvkc0cxMis=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDUwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDYwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASA9qWoAUHr
nn+3kxyNrjPJk82WDLimW21RN51uxpobadv8YgGEDRdP+Ok+uRqQSUsA6ZXfF3iG
r2GjfQ3wMDH8o4GJMIGGMB0GA1UdDgQWBBSjovYaC/m6Li9Tp0V9iZRs9267QzBX
BgNVHSMEUDBOgBTXh06MAV9S4l4lG1TKOrKRBh4qn6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA0ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgcjZNFWJtlDmoPZbAxqsGczRYK0lfPgu6
g1H7pp0ce+wCIDj9BRZM2OB9EF0e+MDKGjyZGfvfrL6Ir47x/KrM6H8T
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDQwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDUwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQEdT0OFf5G
UcrgX2XllCyJzP94NZ464GsgB6psNLsDeL+j7AU+oJy7VLvW/lHh3ODgl08Z9bhq
LFBmNjnHbm8Qo4GJMIGGMB0GA1UdDgQWBBTXh06MAV9S4l4lG1TKOrKRBh4qnzBX
BgNVHSMEUDBOgBQox4F1NsZunlsduoGvzIgRSYfB36EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAzggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAIW++zqDZlLLUk/emePohdNOp5JO3wS9
XvkBJ6Wua7GBAiAdx+EKmdjVrwnzrQltTgnmSfGMXhKNYifK3uD83W3pcQ==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDMwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDQwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQUXDgcUVNT
9hovbZE5HL6rjOb7C55wEuWKThV/CcZ4rWrXx7VXHYdD/R3aDA7JSvYpm2sTok4i
sblDzhZM/GDNo4GJMIGGMB0GA1UdDgQWBBQox4F1NsZunlsduoGvzIgRSYfB3zBX
BgNVHSMEUDBOgBQApzZdtBdD3dLxouQpr/aDiVttd6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAyggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgAkiNhqFAZXSUWEDK91OZvQGdeZOtd6mC
+Wv3fGk3t28CIEKOwidkUTUaiPdZ4efmAr+CEeGzdq27ob2S+nqqHqgV

-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDIwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDMwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQRDXDNIi1p
ereudhqwa2LslXgsxnB63Hu5y5lg+1WPruIYPzD/Ho0APveVdzFLVji19+bE4+tF
PYL1SpsN1WfWo4GJMIGGMB0GA1UdDgQWBBQApzZdtBdD3dLxouQpr/aDiVttdzBX
BgNVHSMEUDBOgBT5RCgQ0AlZTQbfFB2+6+w0XRvydaEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAxggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAOnd+7bAofkHVa4KFNjv3TCegw1lrhuM
8Of8wgvrTEGoAiEAsS8iKMpSfXH4D0egg4gLamE6akde965rDtySU+ve9lg=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDEwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDIwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQWHpv1i6lf
wvNPOP5ka6S0n55EvzoaYK6pbTXP6yMOW/4XZSPKx5Zoq4FMe0cKzGIIFL1rzj1V
2czYB+qvLhyio4GJMIGGMB0GA1UdDgQWBBT5RCgQ0AlZTQbfFB2+6+w0XRvydTBX
BgNVHSMEUDBOgBSh3uHkX5nj86yFEFwjscSWM40P+qEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAI7unGW/gr9tOc3i+dF5N815srgh+FrX
oj9Et74EcSpTAiBubv+vOH0DE0gmYI11HeAIgutWqqMIC72dZlwTF/Vi3g==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB3jCCAYWgAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDAwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQznn9zHHwL
GO8VR4W9V7vMlxCdoojzEOiX5Y6JtPtFOz866ueHY6zoN0/mJ6DnqnSXilJIUUeW
6eGfqmka7nxko4GRMIGOMB0GA1UdDgQWBBSh3uHkX5nj86yFEFwjscSWM40P+jBf
BgNVHSMEWDBWgBQlFYvU5WboI4fcdPoiQs8/fPHZraEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggkA/KCWhcqToHAw
DAYDVR0TBAUwAwEB/zAKBggqhkjOPQQDAgNHADBEAiBasbuinP+pJTU4oDCVD8zQ
1rJBDSOKIEyWu84/D6Hj6wIgVMPUoO01bPhzllAa/gW8Xk/daey09SBgN3AT9pWU
TDA=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIBpTCCAUugAwIBAgIJAPygloXKk6BwMAoGCCqGSM49BAMCMC8xCzAJBgNVBAYT
AlVLMREwDwYDVQQKDAhtYmVkIFRMUzENMAsGA1UEAwwEQ0EwMDAeFw0xNzA2MjIx
MTUwMzJaFw0yNzA2MjMxMTUwMzJaMC8xCzAJBgNVBAYTAlVLMREwDwYDVQQKDAht
YmVkIFRMUzENMAsGA1UEAwwEQ0EwMDBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IA
BFW41/qAwAPpy+Txdc7PKmzZsq9CPiujKU4vpF1ekXnGx2HP420QobwBVVWhkzRm
LwdboH2j65dcCKjQ7mv/dxKjUDBOMB0GA1UdDgQWBBQlFYvU5WboI4fcdPoiQs8/

fPHZrTAfBgNVHSMEGDAWgBQlFYvU5WboI4fcdPoiQs8/fPHZrTAMBgNVHRMEBTAD
AQH/MAoGCCqGSM49BAMCA0gAMEUCIQC7iRcVzwMyfVK5imirJ7MqJQ04euH4CLOt
IZ+SNfaERAIgSU0MWFDosVEIpg8YMqIHeF7Mg4ZyH6+fGazJgVLttUY=
-----END
CERTIFICATE-----

```
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
   <Configuration>Release</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\ssl\ssl_fork_server.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">
    <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid>{918CD402-047D-8467-E11C-E1132053F916}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>ssl_fork_server</RootNamespace>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
```

```
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')"
 Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup
 Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
```

```
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
   <PrecompiledHeader>
   </PrecompiledHeader>
   <WarningLevel>Level3</WarningLevel>
   <Optimization>Disabled</Optimization>

<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
   <SubSystem>Console</SubSystem>
   <GenerateDebugInformation>true</GenerateDebugInformation>
   <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
   <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
   <PrecompiledHeader>
   </PrecompiledHeader>
   <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
   <SubSystem>Console</SubSystem>
   <GenerateDebugInformation>true</GenerateDebugInformation>
   <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
   <LinkLibraryDependencies>false</LinkLibraryDependencies>
```

```
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
   <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
   </PrecompiledHeader>
   <Optimization>MaxSpeed</Optimization>
   <FunctionLevelLinking>true</FunctionLevelLinking>
   <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
   <SubSystem>Console</SubSystem>
   <GenerateDebugInformation>true</GenerateDebugInformation>
   <EnableCOMDATFolding>true</EnableCOMDATFolding>
   <OptimizeReferences>true</OptimizeReferences>
   <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
   <WarningLevel>Level3</WarningLevel>
   <PrecompiledHeader>
   </PrecompiledHeader>
   <Optimization>MaxSpeed</Optimization>
   <FunctionLevelLinking>true</FunctionLevelLinking>
   <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
   <SubSystem>Console</SubSystem>
   <GenerateDebugInformation>true</GenerateDebugInformation>
   <EnableCOMDATFolding>true</EnableCOMDATFolding>
   <OptimizeReferences>true</OptimizeReferences>
   <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
   <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
  <Import Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
```

-----BEGIN CERTIFICATE-----
MIIDwjCCAaqgAwIBAgIBEDANBgkqhkiG9w0BAQsFADBIMQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxJjAkBgNVBAMTHVBvbGFyU1NMIFRlc3QgSW50ZXJt
ZWRpYXRlIENBMB4XDTEzMDkyNDE2MTIyNFoXDTIzMDkyMjE2MTIyNFowNDELMAkG
A1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NMMRIwEAYDVQQDEwlsb2NhbGhvc3Qw
WTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQcbffp2qXqoZyychmoCRxzrd4Vu96m
47NPBehtEC46aTeXgDnBdf++znABrAtfXBRNQz8ARIeYBmskr22rlKjyo4GVMIGS
MAkGA1UdEwQCMAAwHQYDVR0OBBYEFNIK06V3H85VsFxGoo5zbL+hYCa7MGYGA1Ud
IwRfMF2AFDh32Gt3nCh3gotO2BupHveUFrcOoUKkQDA+MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0GC
AQ4wDQYJKoZIhvcNAQELBQADggIBADRoQ5fHKw+vkl0D3aqLX1XrZidb+25AWbhr
FYXdaskN219PrXBL3cV8x5tK6qsPKSyyw1lue80OmhXs/w7PJkOHHUSWRnmTv7lr
8Us3Zr/yOF/VVqzdGs7DlOTpyzEBdugI9uar/aCqHDoltN8wOduOoQB9aojYpROj
+gjlEO0mgt/87XpjYOig1o0jv44QYDQZQzpj1zeIn6WMe6xk9YDwCLMjRIpg++c7
QyxvcEJTn80wX1SaEBM2gau97G7bORLMwBVkMT4oSY+iKYgpPpawOnMJbqUP73Dm
yfJExDdrW/BbWZ/vKIcSqSZIbkHdkNjUDVHczyVwQxZxzvLFw/B1k9s7jYFsi5eK
TNAdXFa4et1H2sd+uhu24GxsjmJioDrftixcgzPVBjDCjH8QWkBEX292WJ58on0e
deWLpZUnzPdE1B4rsiPw1Vg28mGgr2O1xgBQr/fx6A+8ItNTzAXbZfEcult9ypwM
0b6YDNe5IvdKk8iwz3mof0VNy47K6xoCaE/fxxWkjoXK8x2wfswGeP2QgUzQE93b
OtjdHpsG1c7gIVFQmKATyAPUz4vqmezgNRleXU0oL0PYtoCmKQ51UjNMUfmO9xCj
VJaNa2iTQ5Dgic+CW4TYAgj5/9g9X3WfwnDNxrZ0UxxawGElczHXqbrNleTtPaKp
a8Si6UK5
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDgwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDkwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAR7ZB16+t6E
sfahGyKUGJW5mezkzjdaYvc4lbJaKNRwFRfc3F/fmNOSsUFSg/F0N+vUE+doKiPC
8wRwLzvm4s+5o4GJMIGGMB0GA1UdDgQWBBT6gyXHzPIPYc1Vr1aGiLLeMh4HpjBX
BgNVHSMEUDBOgBS40mLt93U8Sh8ZGiDVAhRSiBPcXqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA3ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgO4el1ZPhlIli/qNR2SIEiuvs5Mmy868i
N2Rv5X/VxIECIA/8rUALQxW38XSdBVX3e/jzu7ju47n1YwEqD9K9WdVv
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDUwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDYwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASA9qWoAUHr
nn+3kxyNrjPJk82WDLimW21RN51uxpobadv8YgGEDRdP+Ok+uRqQSUsA6ZXfF3iG
r2GjfQ3wMDH8o4GJMIGGMB0GA1UdDgQWBBSjovYaC/m6Li9Tp0V9iZRs9267QzBX
BgNVHSMEUDBOgBTXh06MAV9S4l4lG1TKOrKRBh4qn6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA0ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgcjZNFWJtlDmoPZbAxqsGczRYK0lfPgu6
g1H7pp0ce+wCIDj9BRZM2OB9EF0e+MDKGjyZGfvfrL6Ir47x/KrM6H8T
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDIwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDMwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQRDXDNIi1p
ereudhqwa2LslXgsxnB63Hu5y5lg+1WPruIYPzD/Ho0APveVdzFLVji19+bE4+tF
PYL1SpsN1WfWo4GJMIGGMB0GA1UdDgQWBBQApzZdtBdD3dLxouQpr/aDiVttdzBX
BgNVHSMEUDBOgBT5RCgQ0AlZTQbfFB2+6+w0XRvydaEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAxggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAOnd+7bAofkHVa4KFNjv3TCegw1lrhuM
8Of8wgvrTEGoAiEAsS8iKMpSfXH4D0egg4gLamE6akde965rDtySU+ve9lg=
-----END CERTIFICATE-----
These certificates form a very long chain, used to test the
MBEDTLS_X509_MAX_INT_CA limit.

NN.key is the private key of certificate NN.crt.

The root is 00.crt and N+1.crt is a child of N.crt.

File cNN.pem contains the chain NN.crt to 00.crt.

Those certificates were generated by tests/data_files/dir-maxpath/long.sh.
-----BEGIN CERTIFICATE-----
MIICHzCCAaWgAwIBAgIBCTAKBggqhkjOPQQDAjA+MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EwHhcN
MTMwOTI0MTU1MjA0WhcNMjMwOTIyMTU1MjA0WjA0MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxEjAQBgNVBAMTCWxvY2FsaG9zdDBZMBMGByqGSM49AgEG
CCqGSM49AwEHA0IABDfMVtl2CR5acj7HWS3/IG7ufPkGkXTQrRS192giWWKSTuUA
2CMR/+ov0jRdXRa9iojCa3cNVc2KKg76Aci07f+jgZ0wgZowCQYDVR0TBAIwADAd
BgNVHQ4EFgQUUGGlj9QH2deCAQzlZX+MY0anE74wbgYDVR0jBGcwZYAUnW0gJEkB
PyvLeLUZvH4kydv7NnyhQqRAMD4xCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQb2xh
clNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBFQyBDQYIJAMFD4n5iQ8zoMAoG
CCqGSM49BAMCA2gAMGUCMQCaLFzXptui5WQN8LlO3ddh1hMxx6tzgLvT03MTVK2S
C12r0Lz3ri/moSEpNZWqPjkCMCE2f53GXcYLqyfyJR078c/xNSUU5+Xxl7VZ414V
fGa5kHvHARBPc8YAIVIqDvHH1Q==
-----END CERTIFICATE-----
RSAES-V15 Encryption Test Vector Int
pkcs1_rsaes_v15_encrypt:1024:16:"bbf82f090682ce9c2338ac2b9da871f7368d07eed41043a440d6b6f07454f51fb8d
fbaaf035c02ab61ea48ceeb6fcd4876ed520d60e1ec4619719d8a5b8b807fafb8e0a3dfc737723ee6b4b7d93a2584ee6a6
49d060953748834b2454598394ee0aab12d7b61a51f527a9a41f6c1687fe2537298ca2a8f5946f8e5fd091dbdcb":16:"1
1":MBEDTLS_MD_SHA1:"d436e99569fd32a7c8a05bbc90d32c49":"aafd12f659cae63489b479e5076ddec2f06cb58
f67c6697351ff4aec29cdbaabf2fbe3467cc254f81be8e78d765a2e63339fc99a66320db73158a35a255d051758e95ed4a
bb2cdc69bb454110e827441213ddc8770e93ea141e1fc673e017e97eadc6b968f385c2aecb03bfb32":"6c5ebca6116b1
e91316613fbb5e93197270a849122d549122d05815e2626f80d20f7f3f038c98295203c0f7f6bb8c3568455c67dec82bc
a86be86eff43b56b7ba2d15375f9a42454c2a2c709953a6e4a977462e35fd21a9c2fb3c0ad2a370f7655267bf6f0481478
4982988e663b869fc8588475af860d499e5a6ffdfc2c6bfd":0

RSAES-V15 Decryption Test Vector Int

pkcs1_rsaes_v15_decrypt:1024:16:"eecfae81b1b9b3c908810b10a1b5600199eb9f44aef4fda493b81a9e3d84f632124ef0236e5d1e3b7e28fae7aa040a2d5b252176459d1f397541ba2a58fb6599":16:"c97fb1f027f453f6341233eaaad1d9353f6c42d08866b1d05a0f2035028b9d869840b41666b42e92ea0da3b43204b5cfce3352524d0416a5a441e700af461503":16:"bbf82f090682ce9c2338ac2b9da871f7368d07eed41043a440d6b6f07454f51fb8dfbaaf035c02ab61ea48ceeb6fcd4876ed520d60e1ec4619719d8a5b8b807fafb8e0a3dfc737723ee6b4b7d93a2584ee6a649d060953748834b2454598394ee0aab12d7b61a51f527a9a41f6c1687fe2537298ca2a8f5946f8e5fd091dbdcb":16:"11":MBEDTLS_MD_SHA1:"d436e99569fd32a7c8a05bbc90d32c49":"aafd12f659cae63489b479e5076ddec2f06cb58f":"28818cb14236ad18f4527e7f1f7633e96cef021bc3234475d7f61e88702b6335b42a352ed3f3267ac7c3e9ba4af17e45096c63eefd8d9a7cb42dfc52fffb2f5b8afb305b46312c2eb50634123b4437a2287ac57b7509d59a583fb741989a49f32625e9267b4641a6607b7303d35c68489db53c8d387b620d0d46a852e72ea43c":0

RSAES-V15

Encryption Test Vector Data just fits

pkcs1_rsaes_v15_encrypt:1024:16:"bbf82f090682ce9c2338ac2b9da871f7368d07eed41043a440d6b6f07454f51fb8dfbaaf035c02ab61ea48ceeb6fcd4876ed520d60e1ec4619719d8a5b8b807fafb8e0a3dfc737723ee6b4b7d93a2584ee6a649d060953748834b2454598394ee0aab12d7b61a51f527a9a41f6c1687fe2537298ca2a8f5946f8e5fd091dbdcb":16:"11":MBEDTLS_MD_SHA1:"4293cecc8095232ae595b84c15ec26f35cf5fde88ae7a9aaa717bcb1ecc4de498da81db97425000770817b5dde5eed01ca3745ff5ab894d0fc0921e5a10b081490129d8ccbaa154ad3dd461397af8ec964ef99402d60a7591ee44b8ce1c16ef88fcb2717076c730d88223893bdd8000b23d87d38ab":"aafd12f659cae63489b479e5076ddec2f06cb58f":"18cdb161f40a18509a3501b7e8ec1c7522e2490319efee8581179b5bcf3750f83a865952d078efd48f58f8060b0d43f9888b43a094fe15209451826ef797195885ff9fa3e26994eee85dbe5dd0404a71565708286027b433c88c85af555b96c34c304dc7c8278233654c022ef340042cfff55e6b15b67cfea8a5a384ef64a6ac":0

RSAES-V15

Decryption Test Vector Data just fits

pkcs1_rsaes_v15_decrypt:1024:16:"eecfae81b1b9b3c908810b10a1b5600199eb9f44aef4fda493b81a9e3d84f632124ef0236e5d1e3b7e28fae7aa040a2d5b252176459d1f397541ba2a58fb6599":16:"c97fb1f027f453f6341233eaaad1d9353f6c42d08866b1d05a0f2035028b9d869840b41666b42e92ea0da3b43204b5cfce3352524d0416a5a441e700af461503":16:"bbf82f090682ce9c2338ac2b9da871f7368d07eed41043a440d6b6f07454f51fb8dfbaaf035c02ab61ea48ceeb6fcd4876ed520d60e1ec4619719d8a5b8b807fafb8e0a3dfc737723ee6b4b7d93a2584ee6a649d060953748834b2454598394ee0aab12d7b61a51f527a9a41f6c1687fe2537298ca2a8f5946f8e5fd091dbdcb":16:"11":MBEDTLS_MD_SHA1:"4293cecc8095232ae595b84c15ec26f35cf5fde88ae7a9aaa717bcb1ecc4de498da81db97425000770817b5dde5eed01ca3745ff5ab894d0fc0921e5a10b081490129d8ccbaa154ad3dd461397af8ec964ef99402d60a7591ee44b8ce1c16ef88fcb2717076c730d88223893bdd8000b23d87d38ab":"aafd12f659cae63489b479e5076ddec2f06cb58f":"18cdb161f40a18509a3501b7e8ec1c7522e2490319efee8581179b5bcf3750f83a865952d078efd48f58f8060b0d43f9888b43a094fe15209451826ef797195885ff9fa3e26994eee85dbe5dd0404a71565708286027b433c88c85af555b96c34c304dc7c8278233654c022ef340042cfff55e6b15b67cfea8a5a384ef64a6ac":0

RSAES-V15

Encryption Test Vector Data too long 1

pkcs1_rsaes_v15_encrypt:1024:16:"bbf82f090682ce9c2338ac2b9da871f7368d07eed41043a440d6b6f07454f51fb8dfbaaf035c02ab61ea48ceeb6fcd4876ed520d60e1ec4619719d8a5b8b807fafb8e0a3dfc737723ee6b4b7d93a2584ee6a649d060953748834b2454598394ee0aab12d7b61a51f527a9a41f6c1687fe2537298ca2a8f5946f8e5fd091dbdcb":16:"11":MBEDTLS_MD_SHA1:"b84293cecc8095232ae595b84c15ec26f35cf5fde88ae7a9aaa717bcb1ecc4de498da81db97425000770817b5dde5eed01ca3745ff5ab894d0fc0921e5a10b081490129d8ccbaa154ad3dd461397af8ec964ef99402d60a7591ee44b8ce1c16ef88fcb2717076c730d88223893bdd8000b23d87d38ab":"aafd12f659cae63489b479e5076ddec2f06cb58f":"05abded6751d620a95177abdba915027b58dd6eecf4ebe71f71c400b115e1d9e12465ace4db3cc03eb57fcbbfe017770f438cf84c10bad505919aefebfa0752087f6376b055beabf0e089fbb90e10f99c795d2d5676eea196db7f9

4a8fd34aedaba39fb230281bb9917cc91793eb37f84dedb2421e9680c39cfda34d4a012134":MBEDTLS_ERR_RSA_BAD_INPUT_DATA

RSAES-V15
Decryption Test Vector Padding too short 7
pkcs1_rsaes_v15_decrypt:1024:16:"eecfae81b1b9b3c908810b10a1b5600199eb9f44aef4fda493b81a9e3d84f632124ef0236e5d1e3b7e28fae7aa040a2d5b252176459d1f397541ba2a58fb6599":16:"c97fb1f027f453f6341233eaaad1d9353f6c42d08866b1d05a0f2035028b9d869840b41666b42e92ea0da3b43204b5cfce3352524d0416a5a441e700af461503":16:"bbf82f090682ce9c2338ac2b9da871f7368d07eed41043a440d6b6f07454f51fb8dfbaaf035c02ab61ea48ceeb6fcd4876ed520d60e1ec4619719d8a5b8b807fafb8e0a3dfc737723ee6b4b7d93a2584ee6a649d060953748834b2454598394ee0aab12d7b61a51f527a9a41f6c1687fe2537298ca2a8f5946f8e5fd091dbdcb":16:"11":MBEDTLS_MD_SHA1:"b84293cecc8095232ae595b84c15ec26f35cf5fde88ae7a9aaa717bcb1ecc4de498da81db97425000770817b5dde5eed01ca3745ff5ab894d0fc0921e5a10b081490129d8ccbaa154ad3dd461397af8ec964ef99402d60a7591ee44b8ce1c16ef88fcb2717076c730d88223893bdd8000b23d87d38ab":"aafd12f659cae63489b479e5076ddec2f06cb58f":"05abded6751d620a95177abdba915027b58dd6eecf4ebe71f71c400b115e1d9e12465ace4db3cc03eb57fcbbfe017770f438cf84c10bad505919aefebfa0752087f6376b055beabf0e089fbb90e10f99c795d2d5676eea196db7f94a8fd34aedaba39fb230281bb9917cc91793eb37f84dedb2421e9680c39cfda34d4a012134":MBEDTLS_ERR_RSA_INVALID_PADDING

RSAES-V15
Encryption Test Vector Data too long 3
pkcs1_rsaes_v15_encrypt:1024:16:"bbf82f090682ce9c2338ac2b9da871f7368d07eed41043a440d6b6f07454f51fb8dfbaaf035c02ab61ea48ceeb6fcd4876ed520d60e1ec4619719d8a5b8b807fafb8e0a3dfc737723ee6b4b7d93a2584ee6a649d060953748834b2454598394ee0aab12d7b61a51f527a9a41f6c1687fe2537298ca2a8f5946f8e5fd091dbdcb":16:"11":MBEDTLS_MD_SHA1:"aa1ab84293cecc8095232ae595b84c15ec26f35cf5fde88ae7a9aaa717bcb1ecc4de498da81db97425000770817b5dde5eed01ca3745ff5ab894d0fc0921e5a10b081490129d8ccbaa154ad3dd461397af8ec964ef99402d60a7591ee44b8ce1c16ef88fcb2717076c730d88223893bdd8000b23d87d38ab":"aafd12f659cae63489b479e5076ddec2f06cb58f":"10d60b8040d57d8701bacb55f2f283d54601ec24d465601ac7f7d5a2f75cac380ba78ca4ab6f3c159f3a9fd6839f5adde0333852ebf876c585664c1a58a1e6885231982f2027be6d7f08ff1807d3ceda8e41ad1f02ddf97a7458832fd13a1f431de6a4ab79e3d4b88bb1df2c5c77fcde9e7b5aa1e7bb29112eae58763127752a":MBEDTLS_ERR_RSA_BAD_INPUT_DATA

RSAES-V15
Decryption Test Vector Padding too short 5
pkcs1_rsaes_v15_decrypt:1024:16:"eecfae81b1b9b3c908810b10a1b5600199eb9f44aef4fda493b81a9e3d84f632124ef0236e5d1e3b7e28fae7aa040a2d5b252176459d1f397541ba2a58fb6599":16:"c97fb1f027f453f6341233eaaad1d9353f6c42d08866b1d05a0f2035028b9d869840b41666b42e92ea0da3b43204b5cfce3352524d0416a5a441e700af461503":16:"bbf82f090682ce9c2338ac2b9da871f7368d07eed41043a440d6b6f07454f51fb8dfbaaf035c02ab61ea48ceeb6fcd4876ed520d60e1ec4619719d8a5b8b807fafb8e0a3dfc737723ee6b4b7d93a2584ee6a649d060953748834b2454598394ee0aab12d7b61a51f527a9a41f6c1687fe2537298ca2a8f5946f8e5fd091dbdcb":16:"11":MBEDTLS_MD_SHA1:"aa1ab84293cecc8095232ae595b84c15ec26f35cf5fde88ae7a9aaa717bcb1ecc4de498da81db97425000770817b5dde5eed01ca3745ff5ab894d0fc0921e5a10b081490129d8ccbaa154ad3dd461397af8ec964ef99402d60a7591ee44b8ce1c16ef88fcb2717076c730d88223893bdd8000b23d87d38ab":"aafd12f659cae63489b479e5076ddec2f06cb58f":"10d60b8040d57d8701bacb55f2f283d54601ec24d465601ac7f7d5a2f75cac380ba78ca4ab6f3c159f3a9fd6839f5adde0333852ebf876c585664c1a58a1e6885231982f2027be6d7f08ff1807d3ceda8e41ad1f02ddf97a7458832fd13a1f431de6a4ab79e3d4b88bb1df2c5c77fcde9e7b5aa1e7bb29112eae58763127752a":MBEDTLS_ERR_RSA_INVALID_PADDING

RSAES-V15

Encryption Test Vector Data too long 8

pkcs1_rsaes_v15_encrypt:1024:16:"bbf82f090682ce9c2338ac2b9da871f7368d07eed41043a440d6b6f07454f51fb8dfbaaf035c02ab61ea48ceeb6fcd4876ed520d60e1ec4619719d8a5b8b807fafb8e0a3dfc737723ee6b4b7d93a2584ee6a649d060953748834b2454598394ee0aab12d7b61a51f527a9a41f6c1687fe2537298ca2a8f5946f8e5fd091dbdcb":16:"11":MBEDTLS_MD_SHA1:"a5a384ef64a6acb84293cecc8095232ae595b84c15ec26f35cf5fde88ae7a9aaa717bcb1ecc4de498da81db97425000770817b5dde5eed01ca3745ff5ab894d0fc0921e5a10b081490129d8ccbaa154ad3dd461397af8ec964ef99402d60a7591ee44b8ce1c16ef88fcb2717076c730d88223893bdd8000b23d87d38ab":"aafd12f659cae63489b479e5076ddec2f06cb58f":"72f98d12ddc230484179ec3022d11b3719222daaa0dc016fc3dbd6771a3f2c9fdd0560f86d616dd50ef1fa5b8c7e1fc40b5abf7b845d7795b3a6af02457b97f783360575cde7497bdf9c104650d4e9a8f4034406de1af95ace39bef2b9e979b74d9a2c0a741d8a21221d9afc98992776cad52d73151613dbc10da9bd8038751a":MBEDTLS_ERR_RSA_BAD_INPUT_DATA

RSAES-V15

Decryption Test Vector Padding too short 0

pkcs1_rsaes_v15_decrypt:1024:16:"eecfae81b1b9b3c908810b10a1b5600199eb9f44aef4fda493b81a9e3d84f632124ef0236e5d1e3b7e28fae7aa040a2d5b252176459d1f397541ba2a58fb6599":16:"c97fb1f027f453f6341233eaaad1d9353f6c42d08866b1d05a0f2035028b9d869840b41666b42e92ea0da3b43204b5cfce3352524d0416a5a441e700af461503":16:"bbf82f090682ce9c2338ac2b9da871f7368d07eed41043a440d6b6f07454f51fb8dfbaaf035c02ab61ea48ceeb6fcd4876ed520d60e1ec4619719d8a5b8b807fafb8e0a3dfc737723ee6b4b7d93a2584ee6a649d060953748834b2454598394ee0aab12d7b61a51f527a9a41f6c1687fe2537298ca2a8f5946f8e5fd091dbdcb":16:"11":MBEDTLS_MD_SHA1:"a5a384ef64a6acb84293cecc8095232ae595b84c15ec26f35cf5fde88ae7a9aaa717bcb1ecc4de498da81db97425000770817b5dde5eed01ca3745ff5ab894d0fc0921e5a10b081490129d8ccbaa154ad3dd461397af8ec964ef99402d60a7591ee44b8ce1c16ef88fcb2717076c730d88223893bdd8000b23d87d38ab":"aafd12f659cae63489b479e5076ddec2f06cb58f":"72f98d12ddc230484179ec3022d11b3719222daaa0dc016fc3dbd6771a3f2c9fdd0560f86d616dd50ef1fa5b8c7e1fc40b5abf7b845d7795b3a6af02457b97f783360575cde7497bdf9c104650d4e9a8f4034406de1af95ace39bef2b9e979b74d9a2c0a741d8a21221d9afc98992776cad52d73151613dbc10da9bd8038751a":MBEDTLS_ERR_RSA_INVALID_PADDING

RSASSA-V15

Signing Test Vector Int

pkcs1_rsassa_v15_sign:1024:16:"d17f655bf27c8b16d35462c905cc04a26f37e2a67fa9c0ce0dced472394a0df743fe7f929e378efdb368eddff453cf007af6d948e0ade757371f8a711e278f6b":16:"c6d92b6fee7414d1358ce1546fb62987530b90bd15e0f14963a5e2635adb69347ec0c01b2ab1763fd8ac1a592fb22757463a982425bb97a3a437c5bf86d03f2f":16:"a2ba40ee07e3b2bd2f02ce227f36a195024486e49c19cb41bbbdfbba98b22b0e577c2eeaffa20d883a76e65e394c69d4b3c05a1e8fadda27edb2a42bc000fe888b9b32c22d15add0cd76b3e7936e19955b220dd17d4ea904b1ec102b2e4de7751222aa99151024c7cb41cc5ea21d00eeb41f7c800834d2c6e06bce3bce7ea9a5":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"859eef2fd78aca00308bdc471193bf55bf9d78db8f8a672b484634f3c9c26e6478ae10260fe0dd8c082e53a5293af2173cd50c6d5d354febf78b26021c25c02712e78cd4694c9f469777e451e7f8e9e04cd3739c6bbfedae487fb55644e9ca74ff77a53cb729802f6ed4a5ffa8ba159890fc":"e3b5d5d002c1bce50c2b65ef88a188d83bce7e61":"2154f928615e5101fcdeb57bc08fc2f35c3d5996403861ae3efb1d0712f8bb05cc21f7f5f11f62e5b6ea9f0f2b62180e5cbe7ba535032d6ac8068fff7f362f73d2c3bf5eca6062a1723d7cfd5abb6dcf7e405f2dc560ffe6fc37d38bee4dc9e24fe2bece3e3b4a3f032701d3f0947b42930083dd4ad241b3309b514595482d42":0

RSASSA-V15

Verification Test Vector Int

pkcs1_rsassa_v15_verify:1024:16:"a2ba40ee07e3b2bd2f02ce227f36a195024486e49c19cb41bbbdfbba98b22b0e577c2eeaffa20d883a76e65e394c69d4b3c05a1e8fadda27edb2a42bc000fe888b9b32c22d15add0cd76b3e7936e19955b220dd17d4ea904b1ec102b2e4de7751222aa99151024c7cb41cc5ea21d00eeb41f7c800834d2c6e06bce3bce7ea9a5":16:"

010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"859eef2fd78aca00308bdc471193bf55bf9d78db8f8a672
b484634f3c9c26e6478ae10260fe0dd8c082e53a5293af2173cd50c6d5d354febf78b26021c25c02712e78cd4694c9f46
9777e451e7f8e9e04cd3739c6bbfedae487fb55644e9ca74ff77a53cb729802f6ed4a5ffa8ba159890fc":"e3b5d5d002c1
bce50c2b65ef88a188d83bce7e61":"2154f928615e5101fcdeb57bc08fc2f35c3d5996403861ae3efb1d0712f8bb05cc2
1f7f5f11f62e5b6ea9f0f2b62180e5cbe7ba535032d6ac8068fff7f362f73d2c3bf5eca6062a1723d7cfd5abb6dcf7e405f2
dc560ffe6fc37d38bee4dc9e24fe2bece3e3b4a3f032701d3f0947b42930083dd4ad241b3309b514595482d42":0
-----BEGIN CERTIFICATE-----
MIIC9zCCAd+gAwIBAgIBATANBgkqhkiG9w0BAQsFADAWMRQwEgYDVQQDEwtUZXN0
IHJvb3QgNDAeFw0wMTAxMDEwMDAwMDBaFw0zMDEyMzEyMzU5NTlaMBYxFDASBgNV
BAMTC1Rlc3Qgcm9vdCA0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
mTX2sHY42Ord9gWyB6GcdlLjjE+4zBJ1BoDpMnvJ89niMTuZTq1ViMp/B6RuTH+2
YF3+riZYQDH9yM/8rgvAUIvK9STaq19Zrm0mnfQUo9yKdkfoJ+XvWuvK6f+NkAMg
xfhAD6eSupigTvov/w2IT8rS0dxo4KF6hKBL2aYlXhiEyi/NmsEPZWvVh+qk3L/Q
GSwpgC+DhVoQzFRofUdK9O9MkgR675iftaFDvyi7F0fxrSLfB/Wy4cgRYzIW6pyN
2sXWivKdLI3bgB01ffdbO17ZAGILK1whO29/bX6hbH09Y/H7jR2vjy+KP9N0PEa3
7SBymlokB3A8wq/LWPYPeQIDAQABo1AwTjAMBgNVHRMEBTADAQEBMB0GA1UdDgQW
BBSOBd1fH00Y9r5S8cELj/9IT4BGlDAfBgNVHSMEGDAWgBSOBd1fH00Y9r5S8cEL
j/9IT4BGlDANBgkqhkiG9w0BAQsFAAOCAQEAWhrHGIMcEG2UJfv920hftxi+Jvj/
ivrhEscqlVA0QNLqZV8v/ai/AiypDLk7uwKtsxF2i+sl81473aSFS9hh3F83/ofm
x8EU8X1FBQHN1zyAEpZyPXr7MiaTXn4w5sCeZLmpWyxGk+cRiPVRE0QUbXDGfVRp
3v984oCUMUzbb+zv6QlkHa6m/kZq0qrnNVVp0X4c7/Pb5elJOVlKnIslNgd/eLrz
zSabToAX9OP6tbJdSRky/LmIYW+CXH/Y4YVwpEu7NisZmDo6lnCBoRQB3QgxoMLp
mM+RUY+AyHr0ZsSUSb6iicJMRZ3mhxCLvnK/Noe/3hq4pUk4Sit7s7JL7A==
-----END
 CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTUwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTYwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQ7Vsp7JmDN
kgPh/+zmIPkd7o0xot/WPMFn3uAsGtsU385MF0fmhfFLhRbbH9h4JjYHj8y0spU3
buUXhftvAZVbo4GJMIGGMB0GA1UdDgQWBBRTw3K0Psy3u/6+3KKSoaQqJnPvPjBX
BgNVHSMEUDBOgBR1mXlrdW5rx1VnqMMnUBXo0WWGWqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTE0ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAMJnGjE9v3SjuGfi0jNByrwyNfhlTHMh
FhPQidNrDpXwAiEAqYtNiV8t9RrAa9GC6FWDuJpvIiU6FsE+lFq6uIq/J2E=
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,BE8274D6692AF2A7

9ZXjoF55A9XgJpdaWmF/ZL1sJfbnE1M42N7HHRDwpq1/K+afC9poM0/AdCUbRL7w
uvQERievbAYpNeLdah1EftM6033e1oTxUMivdL4orDKcbb3qDpSQ0o0UbjavbT+d
aruilW8zVP4dz3mYMvGbkgoujgzdT+4wM0T1mTTuYcRKQsHlg7QDy2QrBILNuXA4
Hmye4GlSXVUSON8vPXT12V4oeubEIZVlnkLTRFGRVA4qz5tby9GBymkeNCBu+LCw
JwJLTbQwMFqozHvioq/2YBaHDcySpTD4X5AwrCjifUNO9BnLWLAmt8dOWr0z+48E
P/yWr5xZl3DrKh9r9EGb9xbTxhum3yHV7bvXLoUH+t9gowmd4Lq3Qjjf8jQXle0P
zoCOVxwN1E1IMhleEUPV7L8mbt26b0JyvrSS5ByrXahGu9vGQyy7qqx9ZANkzgXF

3hPMDuzQXMJiUeG92VsMEdGdA1/8V5ro+ceB5c7Zca5MjMzvx2tihda7BUjj6dSE
cA8Vvksy/NX/nqHSt0aSgphvBmZP8dN6GMcZ+hT7p0fhCq4mSFEykQqueKXiFUfz
0xCUVZC6WzOoEkc8k7xiLWQDlsZZ13Z4yxU1IxJp7llZXpZ8GkwS+678/Nx8h54A
mv5ZlSFWWQrvN5JPQJka7aU2ITu1LUK6mXBu+DoSDOfQuqR4vQytkjOqHK185iHs
JQtBGkFFdElkWgubPX/S8/xxoT8MoQY/c+dr6iwcswyUnSJXh32KLPGNBoqWCCbY
jp/VYmeb117gNpEJKJhcNbrP7DoQrC3/D7JFXnOvTA/z6FOtUmz0rQ==
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIICKzCCAbKgAwIBAgIBLjAKBggqhkjOPQQDAjA+MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EwHhcN
MTQwNDA5MDg0ODUwWhcNMjQwNDA2MDg0ODUwWjA0MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxEjAQBgNVBAMTCWxvY2FsaG9zdDBZMBMGByqGSM49AgEG
CCqGSM49AwEHA0IABDfMVtl2CR5acj7HWS3/IG7ufPkGkXTQrRS192giWWKSTuUA
2CMR/+ov0jRdXRa9iojCa3cNVc2KKg76Aci07f+jgaowgacwCQYDVR0TBAIwADAd
BgNVHQ4EFgQUUGGlj9QH2deCAQzlZX+MY0anE74wbgYDVR0jBGcwZYAUnW0gJEkB
PyvLeLUZvH4kydv7NnyhQqRAMD4xCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQb2xh
clNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBFQyBDQYIJAMFD4n5iQ8zoMAsG
A1UdDwQEAwIDCDAKBggqhkjOPQQDAgNnADBkAjACzKQ88/NvngMQBFc9rC484+gO
BRkXP28BqRcj8sBt3EfmEGH23BuhkZuB1OFZuMICMC4/pHgbOQtaY9WZPUROUVVZ
OuO6XsVbhiE0rb/mumqmUwuOrCtC/KFdvFZol4BNGA==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB5DCCAWmgAwIBAgIBPDAKBggqhkjOPQQDAjA+MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EwHhcN
MTQwNDEwMTcyMTIxWhcNMjQwNDA3MTcyMTIxWjA0MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxEjAQBgNVBAMTCWxvY2FsaG9zdDBZMBMGByqGSM49AgEG
CCqGSM49AwEHA0IABDfMVtl2CR5acj7HWS3/IG7ufPkGkXTQrRS192giWWKSTuUA
2CMR/+ov0jRdXRa9iojCa3cNVc2KKg76Aci07f+jYjBgMAkGA1UdEwQCMAAwHQYD
VR0OBBYEFFBhpY/UB9nXggEM5WV/jGNGpxO+MB8GA1UdIwQYMBaAFJ1tICRJAT8r
y3i1Gbx+JMnb+zZ8MBMGA1UdJQQMMAoGCCsGAQUFBwMCMAoGCCqGSM49BAMCA2kA
MGYCMQCzHyEvd56zm1AzfDBi3psz3rDL/m0RN2WnbRBQJxIJqjwEXOrKazko9m9q
owgau88CMQDuI0fsq5tnyiHPaDSAE21/6hlrCR6deNbwzB94OuPIbx1wIas9D1jc
//iSmKtbl8Y=
-----END CERTIFICATE-----
-----BEGIN EC PARAMETERS-----
BggqhkjOPQMBBw==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIHaMieH2/wn6lnsFUGzww43ymhN16Z0nhG5TyvNeY8U2oAoGCCqGSM49
AwEHoUQDQgAE2cEfliujQRf+64hXTet3PIY2HXWUUeJa81TT8IgUMZ58cKT8qw/Q
Omjz5i3OkqhjiVuGRlQnKCAc3vUSVXogfQ==
-----END EC PRIVATE KEY-----
-----BEGIN CERTIFICATE REQUEST-----
MIICgTCCAWkCAQAwPDELMAkGA1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NMMRow
GAYDVQQDExFQb2xhclNTTCBTZXJ2ZXIgMTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAKkCHz1AatVVU4v9Nu6CZS4VYV6Jv7joRZDb7ogWUtPxQ1BHlhJZ
ZIdr/SvgRvlzvt3PkuGRW+1moG+JKXlFgNCDatVBQ3dfOXwJBEeCsFc5cO2j7BUZ
HqgzCEfBBUKp/UzDtN/dBh9NEFFAZ3MTD0D4bYElXwqxU8YwfhU5rPla7n+SnqYF

W+cTl4W1I5LZ1CQG1QkliXUH3aYajz8JGb6tZSxk65Wb3P5BXhem2mxbacwCuhQs
FiScStzN0PdSZ3PxLaAj/X70McotcMqJCwTbLqZPcG6ezr1YieJTWZ5uWpJl4og/
DJQZo93l6J2VE+0p26twEtxaymsXq1KCVLECAwEAAaAAMA0GCSqGSIb3DQEBDgUA
A4IBAQAed2cYY9P/xJNHBrHDxjeh5uFyDskCvw06Kvy8FJt6G/0ncnfhSpPnevao
UPf2jk07iMIFiaDDKc3yg4H2Uh44+Ud2YdAxHYWttKnvj43XSoWSnmUDEiUqgPAP
C4EmgPEfsxtj+nI5fwIGEvfb3mJ31FJxnSJREcaH8uqyXW4vfF8e0o+9gdM+aTw/
OJj+dYvepfIpB+1jIq1srr9NLJjKlvHBhQFbIcIgQXJKcw5z04hgjdoSuQckMO5z
3gVaaHfjCJQT1tDWfjLTCceDoJPskeo7xbDvXnCho+ZLtyMesoCvOEeZLJhDYTlw
H5jw6f9GW8Q9XP+EQcf6ZhtmYLrU
-----END CERTIFICATE REQUEST-----
-----BEGIN EC PARAMETERS-----
BggqhkjOPQMBBw==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIAzhAcc1Yb2u4bsQDaYeRaRW8kJ/HzFTTfINV1k+TxZ/oAoGCCqGSM49
AwEHoUQDQgAEwxPSz5Sz3IGd29AXIUfwJITRD/RwGr8GGnSSMs6D6OXnQlZ26EB+
/Oo7GcGTWaAtIBwwIQphnCH0XpyEgKFbjw==
-----END EC PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTkwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMjAwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATGebrN8JxE
heOdCxD+mhnQ4zMUxF1WUkmAAHIUw089BYiH9SAwYS/M5tnl+R8fbjvoGqSpR6Tk
V9EU3CQyIoxwo4GJMIGGMB0GA1UdDgQWBBTZs6oChL1c2CSZXY2YFQkkqg+lzDBX
BgNVHSMEUDBOgBRQMc94kTqW+zQO3lo2WMI/81k3c6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTE4ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgRVGZReXKvdMHhwLbPvbrTVLeAGDqmqMH
/WqD4u23QBgCID/QtFaiawjviNFEdtU7JK6v4ZY0PQ0a0+HLZIHLi9ah
-----END CERTIFICATE-----
BLOWFISH-ECB Encrypt SSLeay reference #1
blowfish_encrypt_ecb:"0000000000000000":"0000000000000000":"4ef997456198dd78":0

BLOWFISH-ECB Encrypt SSLeay reference #2
blowfish_encrypt_ecb:"ffffffffffffffff":"ffffffffffffffff":"51866fd5b85ecb8a":0

BLOWFISH-ECB Encrypt SSLeay reference #3
blowfish_encrypt_ecb:"3000000000000000":"1000000000000001":"7d856f9a613063f2":0

BLOWFISH-ECB Encrypt SSLeay reference #4
blowfish_encrypt_ecb:"1111111111111111":"1111111111111111":"2466dd878b963c9d":0

BLOWFISH-ECB Encrypt SSLeay reference #5
blowfish_encrypt_ecb:"0123456789abcdef":"1111111111111111":"61f9c3802281b096":0

BLOWFISH-ECB Encrypt SSLeay reference #6
blowfish_encrypt_ecb:"1111111111111111":"0123456789abcdef":"7d0cc630afda1ec7":0

BLOWFISH-ECB Encrypt SSLeay reference #7
blowfish_encrypt_ecb:"0000000000000000":"0000000000000000":"4ef997456198dd78":0

BLOWFISH-ECB Encrypt SSLeay reference #8
blowfish_encrypt_ecb:"fedcba9876543210":"0123456789abcdef":"0aceab0fc6a0a28d":0

BLOWFISH-ECB Encrypt SSLeay
reference #9
blowfish_encrypt_ecb:"7ca110454a1a6e57":"01a1d6d039776742":"59c68245eb05282b":0

BLOWFISH-ECB Encrypt SSLeay reference #10
blowfish_encrypt_ecb:"0131d9619dc1376e":"5cd54ca83def57da":"b1b8cc0b250f09a0":0

BLOWFISH-ECB Encrypt SSLeay reference #11
blowfish_encrypt_ecb:"07a1133e4a0b2686":"0248d43806f67172":"1730e5778bea1da4":0

BLOWFISH-ECB Encrypt SSLeay reference #12
blowfish_encrypt_ecb:"3849674c2602319e":"51454b582ddf440a":"a25e7856cf2651eb":0

BLOWFISH-ECB Encrypt SSLeay reference #13
blowfish_encrypt_ecb:"04b915ba43feb5b6":"42fd443059577fa2":"353882b109ce8f1a":0

BLOWFISH-ECB Encrypt SSLeay reference #14
blowfish_encrypt_ecb:"0113b970fd34f2ce":"059b5e0851cf143a":"48f4d0884c379918":0

BLOWFISH-ECB Encrypt SSLeay reference #15
blowfish_encrypt_ecb:"0170f175468fb5e6":"0756d8e0774761d2":"432193b78951fc98":0

BLOWFISH-ECB Encrypt SSLeay reference #16
blowfish_encrypt_ecb:"43297fad38e373fe":"762514b829bf486a":"13f04154d69d1ae5":0

BLOWFISH-ECB Encrypt SSLeay reference #17
blowfish_encrypt_ecb:"07a7137045da2a16":"3bdd119049372802":"2eedda93ffd39c79":0

BLOWFISH-ECB
Encrypt SSLeay reference #18
blowfish_encrypt_ecb:"04689104c2fd3b2f":"26955f6835af609a":"d887e0393c2da6e3":0

BLOWFISH-ECB Encrypt SSLeay reference #19
blowfish_encrypt_ecb:"37d06bb516cb7546":"164d5e404f275232":"5f99d04f5b163969":0

BLOWFISH-ECB Encrypt SSLeay reference #20
blowfish_encrypt_ecb:"1f08260d1ac2465e":"6b056e18759f5cca":"4a057a3b24d3977b":0

BLOWFISH-ECB Encrypt SSLeay reference #21
blowfish_encrypt_ecb:"584023641aba6176":"004bd6ef09176062":"452031c1e4fada8e":0

BLOWFISH-ECB Encrypt SSLeay reference #22

blowfish_encrypt_ecb:"025816164629b007":"480d39006ee762f2":"7555ae39f59b87bd":0

BLOWFISH-ECB Encrypt SSLeay reference #23
blowfish_encrypt_ecb:"49793ebc79b3258f":"437540c8698f3cfa":"53c55f9cb49fc019":0

BLOWFISH-ECB Encrypt SSLeay reference #24
blowfish_encrypt_ecb:"4fb05e1515ab73a7":"072d43a077075292":"7a8e7bfa937e89a3":0

BLOWFISH-ECB Encrypt SSLeay reference #25
blowfish_encrypt_ecb:"49e95d6d4ca229bf":"02fe55778117f12a":"cf9c5d7a4986adb5":0

BLOWFISH-ECB
Encrypt SSLeay reference #26
blowfish_encrypt_ecb:"018310dc409b26d6":"1d9d5c5018f728c2":"d1abb290658bc778":0

BLOWFISH-ECB Encrypt SSLeay reference #27
blowfish_encrypt_ecb:"1c587f1c13924fef":"305532286d6f295a":"55cb3774d13ef201":0

BLOWFISH-ECB Encrypt SSLeay reference #28
blowfish_encrypt_ecb:"0101010101010101":"0123456789abcdef":"fa34ec4847b268b2":0

BLOWFISH-ECB Encrypt SSLeay reference #29
blowfish_encrypt_ecb:"1f1f1f1f0e0e0e0e":"0123456789abcdef":"a790795108ea3cae":0

BLOWFISH-ECB Encrypt SSLeay reference #30
blowfish_encrypt_ecb:"e0fee0fef1fef1fe":"0123456789abcdef":"c39e072d9fac631d":0

BLOWFISH-ECB Encrypt SSLeay reference #31
blowfish_encrypt_ecb:"0000000000000000":"ffffffffffffffff":"014933e0cdaff6e4":0

BLOWFISH-ECB Encrypt SSLeay reference #32
blowfish_encrypt_ecb:"ffffffffffffffff":"0000000000000000":"f21e9a77b71c49bc":0

BLOWFISH-ECB Encrypt SSLeay reference #33
blowfish_encrypt_ecb:"0123456789abcdef":"0000000000000000":"245946885754369a":0

BLOWFISH-ECB
Encrypt SSLeay reference #34
blowfish_encrypt_ecb:"fedcba9876543210":"ffffffffffffffff":"6b5c5a9c5d9e0a5a":0

BLOWFISH-ECB Decrypt SSLeay reference #1
blowfish_decrypt_ecb:"0000000000000000":"4ef997456198dd78":"0000000000000000":0

BLOWFISH-ECB Decrypt SSLeay reference #2
blowfish_decrypt_ecb:"ffffffffffffffff":"51866fd5b85ecb8a":"ffffffffffffffff":0

BLOWFISH-ECB Decrypt SSLeay reference #3
blowfish_decrypt_ecb:"3000000000000000":"7d856f9a613063f2":"1000000000000001":0

BLOWFISH-ECB Decrypt SSLeay reference #4
blowfish_decrypt_ecb:"1111111111111111":"2466dd878b963c9d":"1111111111111111":0

BLOWFISH-ECB Decrypt SSLeay reference #5
blowfish_decrypt_ecb:"0123456789abcdef":"61f9c3802281b096":"1111111111111111":0

BLOWFISH-ECB Decrypt SSLeay reference #6
blowfish_decrypt_ecb:"1111111111111111":"7d0cc630afda1ec7":"0123456789abcdef":0

BLOWFISH-ECB Decrypt SSLeay reference #7
blowfish_decrypt_ecb:"0000000000000000":"4ef997456198dd78":"0000000000000000":0

BLOWFISH-ECB
Decrypt SSLeay reference #8
blowfish_decrypt_ecb:"fedcba9876543210":"0aceab0fc6a0a28d":"0123456789abcdef":0

BLOWFISH-ECB Decrypt SSLeay reference #9
blowfish_decrypt_ecb:"7ca110454a1a6e57":"59c68245eb05282b":"01a1d6d039776742":0

BLOWFISH-ECB Decrypt SSLeay reference #10
blowfish_decrypt_ecb:"0131d9619dc1376e":"b1b8cc0b250f09a0":"5cd54ca83def57da":0

BLOWFISH-ECB Decrypt SSLeay reference #11
blowfish_decrypt_ecb:"07a1133e4a0b2686":"1730e5778bea1da4":"0248d43806f67172":0

BLOWFISH-ECB Decrypt SSLeay reference #12
blowfish_decrypt_ecb:"3849674c2602319e":"a25e7856cf2651eb":"51454b582ddf440a":0

BLOWFISH-ECB Decrypt SSLeay reference #13
blowfish_decrypt_ecb:"04b915ba43feb5b6":"353882b109ce8f1a":"42fd443059577fa2":0

BLOWFISH-ECB Decrypt SSLeay reference #14
blowfish_decrypt_ecb:"0113b970fd34f2ce":"48f4d0884c379918":"059b5e0851cf143a":0

BLOWFISH-ECB Encrypt SSLeay reference #15
blowfish_encrypt_ecb:"0170f175468fb5e6":"0756d8e0774761d2":"432193b78951fc98":0

BLOWFISH-ECB
Decrypt SSLeay reference #16
blowfish_decrypt_ecb:"43297fad38e373fe":"13f04154d69d1ae5":"762514b829bf486a":0

BLOWFISH-ECB Decrypt SSLeay reference #17
blowfish_decrypt_ecb:"07a7137045da2a16":"2eedda93ffd39c79":"3bdd119049372802":0

BLOWFISH-ECB Decrypt SSLeay reference #18
blowfish_decrypt_ecb:"04689104c2fd3b2f":"d887e0393c2da6e3":"26955f6835af609a":0

BLOWFISH-ECB Decrypt SSLeay reference #19
blowfish_decrypt_ecb:"37d06bb516cb7546":"5f99d04f5b163969":"164d5e404f275232":0

BLOWFISH-ECB Decrypt SSLeay reference #20
blowfish_decrypt_ecb:"1f08260d1ac2465e":"4a057a3b24d3977b":"6b056e18759f5cca":0

BLOWFISH-ECB Decrypt SSLeay reference #21
blowfish_decrypt_ecb:"584023641aba6176":"452031c1e4fada8e":"004bd6ef09176062":0

BLOWFISH-ECB Decrypt SSLeay reference #22
blowfish_decrypt_ecb:"025816164629b007":"7555ae39f59b87bd":"480d39006ee762f2":0

BLOWFISH-ECB Decrypt SSLeay reference #23
blowfish_decrypt_ecb:"49793ebc79b3258f":"53c55f9cb49fc019":"437540c8698f3cfa":0

BLOWFISH-ECB
Decrypt SSLeay reference #24
blowfish_decrypt_ecb:"4fb05e1515ab73a7":"7a8e7bfa937e89a3":"072d43a077075292":0

BLOWFISH-ECB Decrypt SSLeay reference #25
blowfish_decrypt_ecb:"49e95d6d4ca229bf":"cf9c5d7a4986adb5":"02fe55778117f12a":0

BLOWFISH-ECB Decrypt SSLeay reference #26
blowfish_decrypt_ecb:"018310dc409b26d6":"d1abb290658bc778":"1d9d5c5018f728c2":0

BLOWFISH-ECB Decrypt SSLeay reference #27
blowfish_decrypt_ecb:"1c587f1c13924fef":"55cb3774d13ef201":"305532286d6f295a":0

BLOWFISH-ECB Decrypt SSLeay reference #28
blowfish_decrypt_ecb:"0101010101010101":"fa34ec4847b268b2":"0123456789abcdef":0

BLOWFISH-ECB Decrypt SSLeay reference #29
blowfish_decrypt_ecb:"1f1f1f1f0e0e0e0e":"a790795108ea3cae":"0123456789abcdef":0

BLOWFISH-ECB Decrypt SSLeay reference #30
blowfish_decrypt_ecb:"e0fee0fef1fef1fe":"c39e072d9fac631d":"0123456789abcdef":0

BLOWFISH-ECB Decrypt SSLeay reference #31
blowfish_decrypt_ecb:"0000000000000000":"014933e0cdaff6e4":"ffffffffffffffff":0

BLOWFISH-ECB Decrypt SSLeay
reference #32
blowfish_decrypt_ecb:"ffffffffffffffff":"f21e9a77b71c49bc":"0000000000000000":0

BLOWFISH-ECB Decrypt SSLeay reference #33
blowfish_decrypt_ecb:"0123456789abcdef":"245946885754369a":"0000000000000000":0

BLOWFISH-ECB Decrypt SSLeay reference #34

blowfish_decrypt_ecb:"fedcba9876543210":"6b5c5a9c5d9e0a5a":"ffffffffffffffff":0

BLOWFISH-SETKEY Setkey SSLeay reference #1
blowfish_encrypt_ecb:"f0":"fedcba9876543210":"":MBEDTLS_ERR_BLOWFISH_INVALID_KEY_LENGTH

BLOWFISH-SETKEY Setkey SSLeay reference #2
blowfish_encrypt_ecb:"f0e1":"fedcba9876543210":"":MBEDTLS_ERR_BLOWFISH_INVALID_KEY_LENGTH

BLOWFISH-SETKEY Setkey SSLeay reference #3
blowfish_encrypt_ecb:"f0e1d2":"fedcba9876543210":"":MBEDTLS_ERR_BLOWFISH_INVALID_KEY_LENGTH

BLOWFISH-SETKEY Setkey SSLeay reference #4
blowfish_encrypt_ecb:"f0e1d2c3":"fedcba9876543210":"be1e639408640f05":0

BLOWFISH-SETKEY Setkey SSLeay reference #5
blowfish_encrypt_ecb:"f0e1d2c3b4":"fedcba9876543210":"b39e44481bdb1e6e":0

BLOWFISH-SETKEY Setkey
SSLeay reference #6
blowfish_encrypt_ecb:"f0e1d2c3b4a5":"fedcba9876543210":"9457aa83b1928c0d":0

BLOWFISH-SETKEY Setkey SSLeay reference #7
blowfish_encrypt_ecb:"f0e1d2c3b4a596":"fedcba9876543210":"8bb77032f960629d":0

BLOWFISH-SETKEY Setkey SSLeay reference #8
blowfish_encrypt_ecb:"f0e1d2c3b4a59687":"fedcba9876543210":"e87a244e2cc85e82":0

BLOWFISH-SETKEY Setkey SSLeay reference #9
blowfish_encrypt_ecb:"f0e1d2c3b4a5968778":"fedcba9876543210":"15750e7a4f4ec577":0

BLOWFISH-SETKEY Setkey SSLeay reference #10
blowfish_encrypt_ecb:"f0e1d2c3b4a596877869":"fedcba9876543210":"122ba70b3ab64ae0":0

BLOWFISH-SETKEY Setkey SSLeay reference #11
blowfish_encrypt_ecb:"f0e1d2c3b4a5968778695a":"fedcba9876543210":"3a833c9affc537f6":0

BLOWFISH-SETKEY Setkey SSLeay reference #12
blowfish_encrypt_ecb:"f0e1d2c3b4a5968778695a4b":"fedcba9876543210":"9409da87a90f6bf2":0

BLOWFISH-SETKEY Setkey SSLeay reference #13
blowfish_encrypt_ecb:"f0e1d2c3b4a5968778695a4b3c":"fedcba9876543210":"884f80625060b8b4":0

BLOWFISH-SETKEY
Setkey SSLeay reference #14
blowfish_encrypt_ecb:"f0e1d2c3b4a5968778695a4b3c2d":"fedcba9876543210":"1f85031c19e11968":0

BLOWFISH-SETKEY Setkey SSLeay reference #15

blowfish_encrypt_ecb:"f0e1d2c3b4a5968778695a4b3c2d1e":"fedcba9876543210":"79d9373a714ca34f":0

BLOWFISH-SETKEY Setkey SSLeay reference #16
blowfish_encrypt_ecb:"f0e1d2c3b4a5968778695a4b3c2d1e0f":"fedcba9876543210":"93142887ee3be15c":0

BLOWFISH-SETKEY Setkey SSLeay reference #17
blowfish_encrypt_ecb:"f0e1d2c3b4a5968778695a4b3c2d1e0f00":"fedcba9876543210":"03429e838ce2d14b":0

BLOWFISH-SETKEY Setkey SSLeay reference #18
blowfish_encrypt_ecb:"f0e1d2c3b4a5968778695a4b3c2d1e0f0011":"fedcba9876543210":"a4299e27469ff67b":0

BLOWFISH-SETKEY Setkey SSLeay reference #19
blowfish_encrypt_ecb:"f0e1d2c3b4a5968778695a4b3c2d1e0f001122":"fedcba9876543210":"afd5aed1c1bc96a8":0

BLOWFISH-SETKEY Setkey SSLeay reference #20
blowfish_encrypt_ecb:"f0e1d2c3b4a5968778695a4b3c2d1e0f00112233":"fedcba9876543210":"10851c0e3858da9f":0

BLOWFISH-SETKEY
Setkey SSLeay reference #21
blowfish_encrypt_ecb:"f0e1d2c3b4a5968778695a4b3c2d1e0f0011223344":"fedcba9876543210":"e6f51ed79b9db21f":0

BLOWFISH-SETKEY Setkey SSLeay reference #22
blowfish_encrypt_ecb:"f0e1d2c3b4a5968778695a4b3c2d1e0f001122334455":"fedcba9876543210":"64a6e14afd36b46f":0

BLOWFISH-SETKEY Setkey SSLeay reference #23
blowfish_encrypt_ecb:"f0e1d2c3b4a5968778695a4b3c2d1e0f00112233445566":"fedcba9876543210":"80c7d7d45a5479ad":0

BLOWFISH-SETKEY Setkey SSLeay reference #24
blowfish_encrypt_ecb:"f0e1d2c3b4a5968778695a4b3c2d1e0f0011223344556677":"fedcba9876543210":"05044b62fa52d080":0

BLOWFISH-SETKEY Setkey 440 bits
blowfish_encrypt_ecb:"f0e1d2c3b4a5968778695a4b3c2d1e0f00112233445566778899aabbccddeeff0123456789abcdef0102030405060708090a0b0c0d0e0f":"fedcba9876543210":"9a2ab8f1b00c73d2":0

BLOWFISH-SETKEY Setkey 448 bits
blowfish_encrypt_ecb:"f0e1d2c3b4a5968778695a4b3c2d1e0f00112233445566778899aabbccddeeff0123456789abcdef0102030405060708090a0b0c0d0e0fff":"fedcba9876543210":"2fb3ab7f0ee91b69":0

BLOWFISH-SETKEY
Setkey 456 bits
blowfish_encrypt_ecb:"f0e1d2c3b4a5968778695a4b3c2d1e0f00112233445566778899aabbccddeeff0123456789abcdef0102030405060708090a0b0c0d0e0fffff":"fedcba9876543210":"":MBEDTLS_ERR_BLOWFISH_INVALID_KEY_LENGTH

BLOWFISH-CBC Encrypt
blowfish_encrypt_cbc:"0123456789ABCDEFF0E1D2C3B4A59687":"FEDCBA9876543210":"3736353433323120
4E6F772069732074686520746965206F722000000000":"6b77b4d63006dee605b156e27403979358deb9e7154
616d959f1652bd5ff92cc":0

BLOWFISH-CBC Decrypt
blowfish_decrypt_cbc:"0123456789ABCDEFF0E1D2C3B4A59687":"FEDCBA9876543210":"6B77B4D63006DE
E605B156E27403979358DEB9E7154616D959F1652BD5FF92CC":"37363534333231204e6f772069732074686520
74696d6520666f722000000000":0

BLOWFISH-CBC Encrypt
blowfish_encrypt_cbc:"0123456789ABCDEFF0E1D2C3B4A59687":"FEDCBA9876543210":"3736353433323120
4E6F772069732074686520746965206F7220000000":"":MBEDTLS_ERR_BLOWFISH_INVALID_INPUT_
LENGTH

BLOWFISH-CBC Decrypt
blowfish_decrypt_cbc:"0123456789ABCDEFF0E1D2C3B4A59687":"FEDCBA9876543210":"6B77B4D63006DE
E605B156E27403979358DEB9E7154616D959F1652BD5FF92CC00":"":MBEDTLS_ERR_BLOWFISH_INVALI
D_INPUT_LENGTH

BLOWFISH-CFB
Encrypt
blowfish_encrypt_cfb64:"0123456789ABCDEFF0E1D2C3B4A59687":"FEDCBA9876543210":"37363534333231
204E6F772069732074686520746965206F722000":"e73214a2822139caf26ecf6d2eb9e76e3da3de04d1517200
519d57a6c3"

BLOWFISH-CFB Decrypt
blowfish_decrypt_cfb64:"0123456789ABCDEFF0E1D2C3B4A59687":"FEDCBA9876543210":"E73214A282213
9CAF26ECF6D2EB9E76E3DA3DE04D1517200519D57A6C3":"37363534333231204e6f772069732074686520746
96d6520666f722000"

BLOWFISH-CTR Encrypt
blowfish_encrypt_ctr:"0123456789ABCDEFF0E1D2C3B4A59687":"FEDCBA9876543210":"37363534333231204
E6F772069732074686520746965206F722000":"e73214a2822139ca60254740dd8c5b8acf5e9569c4affeb944b
8fc020e"

BLOWFISH-CTR Decrypt
blowfish_encrypt_ctr:"0123456789ABCDEFF0E1D2C3B4A59687":"FEDCBA9876543210":"e73214a2822139ca6
0254740dd8c5b8acf5e9569c4affeb944b8fc020e":"37363534333231204e6f772069732074686520746965206f7
22000"
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEILBDMs7bRVxVg6ovTpf2zB9m+22jY7R3LNKRvCPfa6YJoAoGCCqGSM49
AwEHoUQDQgAEHG336dql6qGcsnIZqAkcc63eFbvepuOzTwXobRAuOmk3l4A5wXX/
vs5wAawLX1wUTUM/AESHmAZrJK9tq5So8g==
-----END EC PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDIzCCAgsCDFOito4FQA5VXJOV5TANBgkqhkiG9w0BAQsFADBQMRwwGgYDVQQD

ExNQb2xhclNTTCBUZXN0IENBIHYxMRAwDgYDVQQLEwd0ZXN0aW5nMREwDwYDVQQK
EwhQb2xhclNTTDELMAkGA1UEBhMCTkwwIhgPMjAxNDA2MTkxMDA4MTRaGA8yMDI0
MDYxODEwMDgxNFowUDEcMBoGA1UEAxMTUG9sYXJTU0wgVGVzdCBDQSB2MTEQMA4G
A1UECxMHdGVzdGluZzERMA8GA1UEChMIUG9sYXJTU0wxCzAJBgNVBAYTAk5MMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwN83/Be74JadP4beljJ9RKUW
oM0h8ZnU7OrLfBhYCJSl7JvFi98aHpk4mYcee8CNOd84XXB4B9Oe2ZPouXJRxc6j
MFKp8udAcBTLRKJyC8LlQPk+5aYOs/nsSmPAuCkAdJxXO6ilBJBx8b2D2T/WpeI8
Ko/vJ2DDxp/LuuxgfbfmhDK+T/tYJiIDW9S01fv145YucMDkLr38Lu7iQVXANC59
JHJpy0exFECDfWf0hvYxq/F5pLK1LhL5hBfwYm8nPhNYsVQNIZpzN6Ewz2+S3Pbp
/KzbLijRfgJLI6AV8jhlZAnqDG6OGxegccizm8mr6cPyz4eWj4ACMp6ZWG+i1QID
AQABMA0GCSqGSIb3DQEBCwUAA4IBAQBoXC5AlXI5azyOPvmNse2qHhO7BrXOEjH+
9g5P/VsrVADhsUGv6x0A2oLoWXtOjGDIWWH53BWHkCUCu4T5D5C6+I47rXWl4pAr
J+h+tQVZo6J0AJxfPse/NnrjsboUSWhunmo/iTrU6S4KJBguIKP6T1DZoD/8EYgU
x+fXDmvRO+MTesWDiY+p+FHEzsu3b9EBtG9dUiR/zzXi/ktFCfrgstKGSuW6+j7m
lcduTxsogi6Uc3tWKtn6qpSGR0uBoCz6emFO7Smmy/tIyVA88lH0+3UnxOvu4TAK
uvjYkOcZqhprDiMfhxBB7pxbfiviEANTbgSfCtZewSNz2RUJ9ocy
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTYwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTcwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAARrISq2zO9m
D29YCLHB56FdU/RINtRhfeLtM+u5o3HaAnopy0S98RzuEGELjpzr8ZI6kkMMZsj8
nFZQF8HfuE0go4GJMIGGMB0GA1UdDgQWBBSnjWvpWxZcFnfQ2KGtCg/u6fT/DzBX
BgNVHSMEUDBOgBRTw3K0Psy3u/6+3KKSoaQqJnPvPqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTE1ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgDgXjoc6FfMF5W0NziV6vx2BOPNWav01Z
ynEP4h9ULnUCIQC1rU4sEId3UdjzTKhpSGTKtaOuPG+b0YdEMPimI4jmVw==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTUwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTYwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQ7Vsp7JmDN
kgPh/+zmIPkd7o0xot/WPMFn3uAsGtsU385MF0fmhfFLhRbbH9h4JjYHj8y0spU3
buUXhftvAZVbo4GJMIGGMB0GA1UdDgQWBBRTw3K0Psy3u/6+3KKSoaQqJnPvPjBX
BgNVHSMEUDBOgBR1mXlrdW5rx1VnqMMnUBXo0WWGWqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTE0ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAMJnGjE9v3SjuGfi0jNByrwyNfhlTHMh
FhPQidNrDpXwAiEAqYtNiV8t9RrAa9GC6FWDuJpvIiU6FsE+lFq6uIq/J2E=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTQwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTUwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQlKUiMoSss

/hsTasedqdB2BCOGJhTt0hgUGeUnWNZ1svO4yn0GkFHZ08++fl2MKqjpj+VXq0JS
FFyGUOgmgi3Ho4GJMIGGMB0GA1UdDgQWBBR1mXlrdW5rx1VnqMMnUBXo0WWGWjBX
BgNVHSMEUDBOgBRNsJB++ccSBmbCCKBxi4CjXROBk6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTEzggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAKYOIo+fdCQRqpH4LN8qUK1aKzKmWGxS
fGzEEkg/29bMAiAl95cmucoCDMq2Ab8Coc0dEqyJ6+rAPMLBCbGawyiW6A==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTMwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTQwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATRMZN0RHzP
donNmZuq9XPhzvQ52TaokxT39qpQtlFyvUuEGKrLoNvdcpARaA0rGput6RLAQOVU
iNVlJ3Ipj789o4GJMIGGMB0GA1UdDgQWBBRNsJB++ccSBmbCCKBxi4CjXROBkzBX
BgNVHSMEUDBOgBTmVnUSF2MYwws/nCMv7b1wJVkDmqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTEyggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgVfuLpjp08AaxKWf6cuZUUCRd7CojSS1I
71hzeUyFS+sCIQDNJI6P/pBbiHgTaGlBAgfcEfmxmbY0n4xZndtxIkmyVA==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTIwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTMwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATrkzCJLznh
lhnsv1RXB9kfeaD+cIruPQ0cItBDGpdvD8xbBVvQci4+RG2RVUCSWRhkFYjSsUSM
0QHMQnBFlhw2o4GJMIGGMB0GA1UdDgQWBBTmVnUSF2MYwws/nCMv7b1wJVkDmjBX
BgNVHSMEUDBOgBTZTtbi+j0Sm/Zs/+gTkWdASpQzfqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTExggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgWsm+rHJgwUEyNm8EKbEds5yurpp5/3y5
PsvXJVDqxogCIQDUP0Jcl3A907CE2tPVXSgD6LQ6CPu19mixemPw60yijA==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTEwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTIwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATDE9LPlLPc
gZ3b0BchR/AkhNEP9HAavwYadJIyzoPo5edCVnboQH786jsZwZNZoC0gHDAhCmGc
IfRenISAoVuPo4GJMIGGMB0GA1UdDgQWBBTZTtbi+j0Sm/Zs/+gTkWdASpQzfjBX
BgNVHSMEUDBOgBSOSt6ePyMRT6PGMaIi7FqNX9MKtKEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTEwggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgYYF5AnRV7eh2hLD5Dz//pceMTKz9Ls46
E6DxvbfDHikCIFttlGrOCZVyS4ocsjuKIELVUX5qfygI0sn4kU3qCTs2
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G

A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTAwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATZwR+WK6NB
F/7riFdN63c8hjYddZRR4lrzVNPwiBQxnnxwpPyrD9A6aPPmLc6SqGOJW4ZGVCco
IBze9RJVeiB9o4GJMIGGMB0GA1UdDgQWBBSOSt6ePyMRT6PGMaIi7FqNX9MKtDBX
BgNVHSMEUDBOgBQtxZSLJAkEz+2RKMQexM6EtsfgcqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA5ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgN//NqM0FrkrMjmxoeCY9DgxkH2R6sQ4d
NgtwCZAIqEICIBs4vupaVcuvni9tltbP26wi7c0FR+blZuo5DPIA3SVe
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDkwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTAwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAR6jlGKbJd5
hiDxN789gkOcwpyHI9wRwCrADAOwOkMePBPRlwGdm7mw7Z/EAmu26zRm/hcyrs4M
qk2LabDjPI9Xo4GJMIGGMB0GA1UdDgQWBBQtxZSLJAkEz+2RKMQexM6EtsfgcjBX
BgNVHSMEUDBOgBT6gyXHzPIPYc1Vr1aGiLLeMh4HpqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA4ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgP7S8vFstfUBdNe6ym5GYG5Q+aBVEKqRs
fVW7HNUktSYCIQDo6Jua6o/DJbrpq4qYWq5gv4yGyzPTN+3IaKrEICdaaw==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDgwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDkwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAR7ZB16+t6E
sfahGyKUGJW5mezkzjdaYvc4lbJaKNRwFRfc3F/fmNOSsUFSg/F0N+vUE+doKiPC
8wRwLzvm4s+5o4GJMIGGMB0GA1UdDgQWBBT6gyXHzPIPYc1Vr1aGiLLeMh4HpjBX
BgNVHSMEUDBOgBS40mLt93U8Sh8ZGiDVAhRSiBPcXqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA3ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgO4el1ZPhlIli/qNR2SIEiuvs5Mmy868i
N2Rv5X/VxIECIA/8rUALQxW38XSdBVX3e/jzu7ju47n1YwEqD9K9WdVv
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDcwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDgwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAARpQeQ/YGQj
nl7Szo6WStJ1u7xunTL5jBkXH8aAVSm0qiX4AD/7YPxa5EnGzZdLTn25vQVnfQAG
pMx8P1lYiGYCo4GJMIGGMB0GA1UdDgQWBBS40mLt93U8Sh8ZGiDVAhRSiBPcXjBX
BgNVHSMEUDBOgBREq5J3toJPxZ3O+ssJ5vkkU0RJE6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA2ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhANwGf+F4a+kmXWz8UjSpRkaToTV6EFWw
/Tjzj0tQhDoAAiEA19RxeWOVBBpM6LOHg6v5Lf54YN1snkLf+sEXyZCuWQQ=
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDYwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDcwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASNOj4d4MEA
7p/3miijqG4ToE4opKPAm+3BTIGrJTYT14++TSiUICl0ASXj+xeUcLMIaXTN042s
LsHxpShzQaL0o4GJMIGGMB0GA1UdDgQWBBREq5J3toJPxZ3O+ssJ5vkkU0RJEzBX
BgNVHSMEUDBOgBSjovYaC/m6Li9Tp0V9iZRs9267Q6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA1ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAKGcf+c442c/XiwubbaiQvsoZ7EoVxuM
oKmia0gPyBNkAiEA83asjJ5FDXQuLyZpczviXrbmqgCPOfYadtvkc0cxMis=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDUwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDYwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASA9qWoAUHr
nn+3kxyNrjPJk82WDLimW21RN51uxpobadv8YgGEDRdP+Ok+uRqQSUsA6ZXfF3iG
r2GjfQ3wMDH8o4GJMIGGMB0GA1UdDgQWBBSjovYaC/m6Li9Tp0V9iZRs9267QzBX
BgNVHSMEUDBOgBTXh06MAV9S4l4lG1TKOrKRBh4qn6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA0ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgcjZNFWJtlDmoPZbAxqsGczRYK0lfPgu6
g1H7pp0ce+wCIDj9BRZM2OB9EF0e+MDKGjyZGfvfrL6Ir47x/KrM6H8T
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDQwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDUwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQEdT0OFf5G
UcrgX2XllCyJzP94NZ464GsgB6psNLsDeL+j7AU+oJy7VLvW/lHh3ODgl08Z9bhq
LFBmNjnHbm8Qo4GJMIGGMB0GA1UdDgQWBBTXh06MAV9S4l4lG1TKOrKRBh4qnzBX
BgNVHSMEUDBOgBQox4F1NsZunlsduoGvzIgRSYfB36EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAzggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAIW++zqDZlLLUk/emePohdNOp5JO3wS9
XvkBJ6Wua7GBAiAdx+EKmdjVrwnzrQltTgnmSfGMXhKNYifK3uD83W3pcQ==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDMwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDQwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQUXDgcUVNT
9hovbZE5HL6rjOb7C55wEuWKThV/CcZ4rWrXx7VXHYdD/R3aDA7JSvYpm2sTok4i
sblDzhZM/GDNo4GJMIGGMB0GA1UdDgQWBBQox4F1NsZunlsduoGvzIgRSYfB3zBX
BgNVHSMEUDBOgBQApzZdtBdD3dLxouQpr/aDiVttd6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAyggEBMAwGA1UdEwQF

MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgAkiNhqFAZXSUWEDK91OZvQGdeZOtd6mC
+Wv3fGk3t28CIEKOwidkUTUaiPdZ4efmAr+CEeGzdq27ob2S+nqqHqgV
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDIwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDMwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQRDXDNIi1p
ereudhqwa2LslXgsxnB63Hu5y5lg+1WPruIYPzD/Ho0APveVdzFLVji19+bE4+tF
PYL1SpsN1WfWo4GJMIGGMB0GA1UdDgQWBBQApzZdtBdD3dLxouQpr/aDiVttdzBX
BgNVHSMEUDBOgBT5RCgQ0AlZTQbfFB2+6+w0XRvydaEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAxggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAOnd+7bAofkHVa4KFNjv3TCegw1lrhuM
8Of8wgvrTEGoAiEAsS8iKMpSfXH4D0egg4gLamE6akde965rDtySU+ve9lg=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDEwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDIwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQWHpv1i6lf
wvNPOP5ka6S0n55EvzoaYK6pbTXP6yMOW/4XZSPKx5Zoq4FMe0cKzGIIFL1rzj1V
2czYB+qvLhyio4GJMIGGMB0GA1UdDgQWBBT5RCgQ0AlZTQbfFB2+6+w0XRvydTBX
BgNVHSMEUDBOgBSh3uHkX5nj86yFEFwjscSWM40P+qEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAI7unGW/gr9tOc3i+dF5N815srgh+FrX
oj9Et74EcSpTAiBubv+vOH0DE0gmYI11HeAIgutWqqMIC72dZlwTF/Vi3g==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB3jCCAYWgAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDAwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQznn9zHHwL
GO8VR4W9V7vMlxCdoojzEOiX5Y6JtPtFOz866ueHY6zoN0/mJ6DnqnSXilJIUUeW
6eGfqmka7nxko4GRMIGOMB0GA1UdDgQWBBSh3uHkX5nj86yFEFwjscSWM40P+jBf
BgNVHSMEWDBWgBQlFYvU5WboI4fcdPoiQs8/fPHZraEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggkA/KCWhcqToHAw
DAYDVR0TBAUwAwEB/zAKBggqhkjOPQQDAgNHADBEAiBasbuinP+pJTU4oDCVD8zQ
1rJBDSOKIEyWu84/D6Hj6wIgVMPUoO01bPhzllAa/gW8Xk/daey09SBgN3AT9pWU
TDA=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIBpTCCAUugAwIBAgIJAPygloXKk6BwMAoGCCqGSM49BAMCMC8xCzAJBgNVBAYT
AlVLMREwDwYDVQQKDAhtYmVkIFRMUzENMAsGA1UEAwwEQ0EwMDAeFw0xNzA2MjIx
MTUwMzJaFw0yNzA2MjMxMTUwMzJaMC8xCzAJBgNVBAYTAlVLMREwDwYDVQQKDAht
YmVkIFRMUzENMAsGA1UEAwwEQ0EwMDBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IA
BFW41/qAwAPpy+Txdc7PKmzZsq9CPiujKU4vpF1ekXnGx2HP420QobwBVVWhkzRm

```
LwdboH2j65dcCKjQ7mv/dxKjUDBOMB0GA1UdDgQWBBQlFYvU5WboI4fcdPoiQs8/
fPHZrTAfBgNVHSMEGDAWgBQlFYvU5WboI4fcdPoiQs8/fPHZrTAMBgNVHRMEBTAD
AQH/MAoGCCqGSM49BAMCA0gAMEUCIQC7iRcVzwMyfVK5imirJ7MqJQ04euH4CLOt
IZ+SNfaERAIgSU0MWFDosVEIpg8YMqIHeF7Mg4ZyH6+fGazJgVLttUY=
-----END
 CERTIFICATE-----
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
   <Configuration>Release</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\pkey\rsa_sign_pss.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">
    <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid>{DCD3A1B6-5EC1-8266-93EF-BD2B9BEFE12D}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>rsa_sign_pss</RootNamespace>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
```

```
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
/>
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
```

```
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
   <PrecompiledHeader>
   </PrecompiledHeader>
   <WarningLevel>Level3</WarningLevel>
   <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
    <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
   <SubSystem>Console</SubSystem>
   <GenerateDebugInformation>true</GenerateDebugInformation>
   <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
   <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
   <PrecompiledHeader>
   </PrecompiledHeader>
   <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
 <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
   <SubSystem>Console</SubSystem>
   <GenerateDebugInformation>true</GenerateDebugInformation>
   <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
   <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
```

```
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
  </Link>
 </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
  <Import Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
```

README for git hooks script
==========

git has a way to run scripts, which are invoked by specific git commands.
The git hooks are located in `<mbed TLS root>/.git/hooks`, and as such are not under version control
for more information, see the [git documentation](https://git-scm.com/docs/githooks).

The mbed TLS git hooks are located in `<mbed TLS root>/tests/git-scripts` directory, and one must create a soft link from `<mbed TLS root>/.git/hooks` to `<mbed TLS root>/tesst/git-scripts`, in order to make the hook scripts successfully work.

Example:

Execute the following command to create a link on linux from the mbed TLS `.git/hooks` directory:
`ln -s ../../tests/git-scripts/pre-push.sh pre-push`

Note: Currently the mbed TLS git hooks work only on a GNU platform. If using a non-GNU platform, don't enable these hooks!

These scripts can also be used independently.
-----BEGIN EC PRIVATE KEY-----
MIGoAgEBBDA92S51DZDX05/BiFzYrRLqlEHyK5M0tNllICrbFEjOJMWAioXdmvwi
mvCjEk91W8ugCwYJKyQDAwIIAQELoWQDYgAEcZ+dCTpifg01A4XGYc6/AMYZI1Zv
6QBqMQevHYcbxrtomF/XIuoyvjFvjng7fNGVd4X2bPwMsZXdXJmo56uqhIVTpYTf
0rSOdtRF/gDdi+WQlth31GltI7S8jbFHJOZq
-----END EC PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDCjCCAfKgAwIBAgIBATANBgkqhkiG9w0BAQsFADAmMSQwIgYDVQQDExtUZXN0
IGludGVybWVkaWF0ZSBtYXhwYXRoIDEwHhcNMDEwMTAxMDAwMDAwWhcNMzAxMjMx
MjM1OTU5WjAcMRowGAYDVQQDExFUZXN0IExlYWYgdmFsaWQgMjCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAIoBoBxjVjZBFlhZ+3mlOJAtlo0d0bXAbKFt
TJUJ3VL8FlB4HG3yIO54eujoul5dyKgDIx49SdBDxnME35i3Wkbzd/Co0zId/xYh
a61C9DDYIhsY5E7YVoLH1eAv4t70Q0wlvtlDBXXevs+4cBX/pXU7Aj/UKfvdxna7
Ja7wEdltKoxy1CwCRpP+ls8RRusXgoHYZKKAz6a7H5WSf3DdUrqk2DmlTAI/SWqL
0rVE1YRfKLg1C6atH4gSJqJXTm3BnWgFpYEZdJPDXaEi6Vnf+/oYuLB+T0jmavvI
NZUN3IKxO7WuF96f4ungKXJ9YchJE8vWaSjhb2V5zOA9Y/PikikCAwEAAaNNMEsw
CQYDVR0TBAIwADAdBgNVHQ4EFgQUwjdrwy2NbXHp088kZpUuEwXtsYowHwYDVR0j
BBgwFoAUOBl8edVm/H5xdS2EGEeLzftZ/DUwDQYJKoZIhvcNAQELBQADggEBABrt
2fKOUwAb5EFD/ebXMM4Qzg6sFYpq/mcnPlmGmqwNzmumlgYUBS15liTnA4nBgR09
b2sejlwnzcnrsFB18YCmE/TIPuh3XMJXmUxjcnCy3qPuSwpuwG3brUGQPiIZhRZz
1+iSc7uba/JGaTqLBItaRPlB6dD3jqY3UowFaWvnYiVmCXg147EBC5Mn2EDiukg0
xsqM03yfpUkp4/W9+WpJuGNyhicSJbNxlh3zEjrgWeMvhnFmrTr7ss6P2ZoKGS3/
QrZBLUzkk25hCF3dTNfTDVSQUt0rONJvx3ym+Kp+zQWc/oHsDs0STs5Db2J0dGp8
VEyxyevfwivF4EQ70Jw=
-----END
 CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIC6zCCAnKgAwIBAgIBETAKBggqhkjOPQQDAjBLMQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxKTAnBgNVBAMTIFBvbGFyU1NMIFRlc3QgSW50ZXJtZWRp

YXRlIEVDIENBMB4XDTEzMDkyNDE2MTI1NloXDTIzMDkyMjE2MTI1NlowNDELMAkG
A1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NMMRIwEAYDVQQDEwlsb2NhbGhvc3Qw
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDbHH8uC82/ztF1EKCiuM59
quIF4HrYRGOPtb3AsBm5N7gZSg7xXXSAZ0aHBt5bfwYDvcGNXgcV1Fv03OXPPfnB
ESyuarmKvR1nZhfqTr3bFZqCh+TweMOjhYew/Z+pmV/jM+zM6gu1YV7xSX4/oy3q
AQzMQpp2m8TQN9OxFwFhARZZfhwXw1P90XLLTGAV2n3i6q1Q747ii9Rqd1XWcNlr
u/HuOQQ4o73i0eBma+KcR5npKOa2/C7KZ0OE6NWD1p2YawE+gdw8esr585z31igb
J3h8w9DVY6eBNImtJWq98urt+lf85TTGwQ9xLdIIEButREHg/nmgY5OKsV3psO5v
AgMBAAGjgZIwgY8wCQYDVR0TBAIwADAdBgNVHQ4EFgQU4j/mLfTnuKaM3G0XpxhA
J2F2Dx0wYwYDVR0jBFwwWoAUD4m9Y0Hry14XKP9oMD3BiNCcWDmhP6Q9MDsxCzAJ
BgNVBAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEZMBcGA1UEAxMQUG9sYXJTU0wg
VGVzdCBDQYIBDzAKBggqhkjOPQQDAgNnADBkAjBkP1bGlZvxnYySZjdBq4m8lkyz
2cjfqjYs8COEkRkONaVz7888HvFdGpL98uQeFvECMHCyCrHprkGzvq/L9kUnx9Bh
2IHbCzbbi9moYC1XcOxgfsEKmhtVF/uQdf8+3VtGqA==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIC6TCCAdGgAwIBAgIBDzANBgkqhkiG9w0BAQsFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTMwOTI0MTYwODQyWhcNMjMwOTIyMTYwODQyWjBLMQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxKTAnBgNVBAMTIFBvbGFyU1NMIFRlc3QgSW50ZXJtZWRp
YXRlIEVDIENBMHYwEAYHKoZIzj0CAQYFK4EEACIDYgAE8Oih3fX5SLeN1dmFncQl
WMw9+Y6sXblhlrXBxhXxjwdwpCHENn+foUVdrqYVYa7Suv3QVeO6nJ19H3QNixW8
ik1P+hxsbaq8bta78vAyHmC4EmXQLg1w7oxb9Q82qX1Yo4GVMIGSMB0GA1UdDgQW
BBQPib1jQevLXhco/2gwPcGI0JxYOTBjBgNVHSMEXDBagBS0WuSls97SUva51aaV
D+s+vMf9/6E/pD0wOzELMAkGA1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NMMRkw
FwYDVQQDExBQb2xhclNTTCBUZXN0IENBggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZI
hvcNAQELBQADggEBAAjeaTUaCBiXT1CYLVr6UFSeRNZBrDPnj6PwqUQTvgB5I5n6
yXqoE4RYDaEL0Lg24juFxI26itBuypto6vscgGq77cfrP/avSdxU+xeZ4bCWvh3M
ddj9lmko2U8I8GhBcHpSuIiTvgKDB8eKkjeq3AsLGchHDvip8pB3IhcNfL7W94Zf
7/lH9VQiE3/px7amD32cidoPvWLA9U3f1FsPmJESUz0wwNfINpDjmPr8dGbkCN+M
CFhxo6sCfK8KLYG4nYX8FwxVR86kpSrO9e84AX0YYbdzxprbc2XOaebJ8+BDmzut
ARkD7DTXrodN1wV7jQJkrUuEwPj9Rhvk+MFRkaw=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDQwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDUwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQEdT0OFf5G
UcrgX2XllCyJzP94NZ464GsgB6psNLsDeL+j7AU+oJy7VLvW/lHh3ODgl08Z9bhq
LFBmNjnHbm8Qo4GJMIGGMB0GA1UdDgQWBBTXh06MAV9S4l4lG1TKOrKRBh4qnzBX
BgNVHSMEUDBOgBQox4F1NsZunlsduoGvzIgRSYfB36EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAzggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAIW++zqDZlLLUk/emePohdNOp5JO3wS9
XvkBJ6Wua7GBAiAdx+EKmdjVrwnzrQltTgnmSfGMXhKNYifK3uD83W3pcQ==
-----END CERTIFICATE-----

-----BEGIN X509 CRL-----
MIIBcTCB9wIBATAKBggqhkjOPQQDBDA+MQswCQYDVQQGEwJOTDERMA8GA1UEChMI
UG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EXDTEzMDkyNDE2
MzEwOFoXDTIzMDkyMjE2MzEwOFowFDASAgEKFw0xMzA5MjQxNjI4MzhaoHIwcDBu
BgNVHSMEZzBlgBSdbSAkSQE/K8t4tRm8fiTJ2/s2fKFCpEAwPjELMAkGA1UEBhMC
TkwxETAPBgNVBAoTCFBvbGFyU1NMMRwwGgYDVQQDExNQb2xhcnNzbCBUZXN0IEVD
IENBggkAwUPifmJDzOgwCgYIKoZIzj0EAwQDaQAwZgIxAL/VFrDIYUECsS0rVpAy
6zt/CqeAZ1sa/l5LTaG1XW286n2Kibipr6EpkYZNYIQILgIxAI0wb3Py1DHPWpYf
/BFBH7C3KYq+nWTrLeEnhrjU1LzG/CiQ8lnuskya6lw/P3lJ/A==
-----END X509 CRL-----
-----BEGIN CERTIFICATE-----
MIIDijCCAnKgAwIBAgIBLDANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTQwNDA5MDg0NDUxWhcNMjQwNDA2MDg0NDUxWjA0MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxEjAQBgNVBAMTCWxvY2FsaG9zdDCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBAMFNo93nzR3RBNdJcriZrA545Do8Ss86ExbQWuTN
owCIp+4ea5anUrSQ7y1yej4kmvy2NKwk9XfgJmSMnLAofaHa6ozmyRyWvP7BBFKz
NtSj+uGxdtiQwWG0ZlI2oiZTqqt0Xgd9GYLbKtgfoNkNHC1JZvdbJXNG6AuKT2kM
tQCQ4dqCEGZ9rlQri2V5kaHiYcPNQEkI7mgM8YuG0ka/0LiqEQMef1aoGh5EGA8P
hYvai0Re4hjGYi/HZo36Xdh98yeJKQHFkA4/J/EwyEoO79bex8cna8cFPXrEAjya
HT4P6DSYW8tzS1KW2BGiLICIaTla0w+w3lkvEcf36hIBMJcCAwEAAaOBnzCBnDAJ
BgNVHRMEAjAAMB0GA1UdDgQWBBSlBehkuNzfYA9QEk1gqGSvTYtDkzBjBgNVHSME
XDBagBS0WuSls97SUva51aaVD+s+vMf9/6E/pD0wOzELMAkGA1UEBhMCTkwxETAP
BgNVBAoTCFBvbGFyU1NMMRkwFwYDVQQDExBQb2xhclNTTCBUZXN0IENBggEAMAsG
A1UdDwQEAwIHgDANBgkqhkiG9w0BAQUFAAOCAQEAc4kubASrFXFtplkYp6FUcnUn
Pf/6laS1htI+3y+q1UHWe2PcagZtCHTCUGBSWLeUIiaIBheaIRqv+4sSFVuXB7hV
0PGXpO5btth4R8BHzGqCdObKvPujp5BDq3xgcAFicA3HUMNsJoTDv/RYXY7je1Q5
ntVyVPeji0AWMUYQjcqHTQQPGBgdJrRTMaYglZh15IhJ16ICNd9rWIeBA0h/+r0y
QuFEBz0nfe7Dvpqct7gJCv+7/5tCujx4LT17z7oK8BZN5SePAGU2ykJsUXk8ZICT
ongaQQVQwS6/GJ6A5V8ecaUvFrTby1h9+2sOW8n2NRGiaaG5gkvxVeayemcmOQ==
-----END
 CERTIFICATE-----
This directory contains example configuration files.

The examples are generally focused on a particular usage case (eg, support for
a restricted number of ciphersuites) and aim at minimizing resource usage for
this target. They can be used as a basis for custom configurations.

These files are complete replacements for the default config.h. To use one of
them, you can pick one of the following methods:

1. Replace the default file include/mbedtls/config.h with the chosen one.
  (Depending on your compiler, you may need to ajust the line with
  #include "mbedtls/check_config.h" then.)

2. Define MBEDTLS_CONFIG_FILE and adjust the include path accordingly.
  For example, using make:

CFLAGS="-I$PWD/configs -DMBEDTLS_CONFIG_FILE='<foo.h>'" make

Or, using cmake:

find . -iname '*cmake*' -not -name CMakeLists.txt -exec rm -rf {} +
CFLAGS="-I$PWD/configs -DMBEDTLS_CONFIG_FILE='<foo.h>'" cmake .
make

Note that the second method also works if you want to keep your custom
configuration
file outside the mbed TLS tree.
-----BEGIN CERTIFICATE-----
MIICKzCCAbKgAwIBAgIBLzAKBggqhkjOPQQDAjA+MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EwHhcN
MTQwNDA5MDg0OTA0WhcNMjQwNDA2MDg0OTA0WjA0MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxEjAQBgNVBAMTCWxvY2FsaG9zdDBZMBMGByqGSM49AgEG
CCqGSM49AwEHA0IABDfMVtl2CR5acj7HWS3/IG7ufPkGkXTQrRS192giWWKSTuUA
2CMR/+ov0jRdXRa9iojCa3cNVc2KKg76Aci07f+jgaowgacwCQYDVR0TBAIwADAd
BgNVHQ4EFgQUUGlj9QH2deCAQzlZX+MY0anE74wbgYDVR0jBGcwZYAUnW0gJEkB
PyvLeLUZvH4kydv7NnyhQqRAMD4xCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQb2xh
clNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBFQyBDQYIJAMFD4n5iQ8zoMAsG
A1UdDwQEAwIFIDAKBggqhkjOPQQDAgNnADBkAjAMl0Cjv9f45bHeJTul5XpYeJeT
52ZaOLTa/uTLy948EnEIi6sj3nFb9fvsUbsOOjECMAXAMY64KOqzixefz3y3XS/d
9miyeArPOmXU2JJ3LGuNbqqj9IbABawB1OD8v8gRmg==
-----END CERTIFICATE-----
AES-128-CFB128 Encrypt NIST KAT #1
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"f0000000000000000000000000000000":"00000000000000000000000000000000":"00000000
000000000000000000000000":"970014d634e2b7650777e8e84d03ccd8"

AES-128-CFB128 Encrypt NIST KAT #2
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"f8000000000000000000000000000000":"00000000000000000000000000000000":"00000000
000000000000000000000000":"f17e79aed0db7e279e955b5f493875a7"

AES-128-CFB128 Encrypt NIST KAT #3
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"fc0000000000000000000000000000":"00000000000000000000000000000000":"00000000
000000000000000000000000":"9ed5a75136a940d0963da379db4af26a"

AES-128-CFB128 Encrypt NIST KAT #4
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"64cf9c7abc50b888af65f49d521944b2":"00000000000000000000000000000000":"00000000
000000000000000000000000":"f7efc89d5dba578104016ce5ad659c05"

AES-128-CFB128 Encrypt NIST KAT #5
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"47d6742eefcc0465dc96355e851b64d9":"00000000000000000000000000000000":"00000000

00000000000000000000000":"0306194f666d183624aa230a8b264ae7"

AES-128-CFB128
Encrypt NIST KAT #6
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"3eb39790678c56bee34bbcdeccf6cdb5":"00000000000000000000000000000000":"00000000000000000000000000000000":"858075d536d79ccee571f7d7204b1f67"

AES-128-CFB128 Encrypt NIST KAT #7
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"00000000000000000000000000000000":"6a118a874519e64e9963798a503f1d35":"00000000000000000000000000000000":"dc43be40be0e53712f7e2bf5ca707209"

AES-128-CFB128 Encrypt NIST KAT #8
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"00000000000000000000000000000000":"cb9fceec81286ca3e989bd979b0cb284":"00000000000000000000000000000000":"92beedab1895a94faa69b632e5cc47ce"

AES-128-CFB128 Encrypt NIST KAT #9
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"00000000000000000000000000000000":"b26aeb1874e47ca8358ff22378f09144":"00000000000000000000000000000000":"459264f4798f6a78bacb89c15ed3d601"

AES-128-CFB128
Encrypt NIST KAT #10
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"00000000000000000000000000000000":"ffffffffffffffffffffffffffffffff0":"00000000000000000000000000000000":"f9b0fda0c4a898f5b9e6f661c4ce4d07"

AES-128-CFB128 Encrypt NIST KAT #11
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"00000000000000000000000000000000":"ffffffffffffffffffffffffffffff8":"00000000000000000000000000000000":"8ade895913685c67c5269f8aae42983e"

AES-128-CFB128 Encrypt NIST KAT #12
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"00000000000000000000000000000000":"ffffffffffffffffffffffffffffffc":"00000000000000000000000000000000":"39bde67d5c8ed8a8b1c37eb8fa9f5ac0"

AES-128-CFB128 Decrypt NIST KAT #1
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"fffffffe00000000000000000000000":"00000000000000000000000000000000":"1114bc2028009b923f0b01915ce5e7c4":"00000000000000000000000000000000"

AES-128-CFB128
Decrypt NIST KAT #2
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"fffffff00000000000000000000000":"00000000000000000000000000000000":"9c28524a16

a1e1c1452971caa8d13476":"00000000000000000000000000000000"

AES-128-CFB128 Decrypt NIST KAT #3
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"ffffffff80000000000000000000000":"00000000000000000000000000000000":"ed62e16363638360fdd6ad62112794f0":"00000000000000000000000000000000"

AES-128-CFB128 Decrypt NIST KAT #4
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"3071a2a48fe6cbd04f1a129098e308f8":"00000000000000000000000000000000":"4b98e06d356deb07ebb824e5713f7be3":"00000000000000000000000000000000"

AES-128-CFB128 Decrypt NIST KAT #5
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"90f42ec0f68385f2ffc5dfc03a654dce":"00000000000000000000000000000000":"7a20a53d460fc9ce0423a7a0764c6cf2":"00000000000000000000000000000000"

AES-128-CFB128 Decrypt NIST KAT #6
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"febd9a24d8b65c1c787d50a4ed3619a9":"00000000000000000000000000000000":"f4a70d8af877f9b02b4c40df57d45b17":"00000000000000000000000000000000"

AES-128-CFB128
Decrypt NIST KAT #7
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"00000000000000000000000000000000":"f34481ec3cc627bacd5dc3fb08f273e6":"0336763e966d92595a567cc9ce537f5e":"00000000000000000000000000000000"

AES-128-CFB128 Decrypt NIST KAT #8
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"00000000000000000000000000000000":"9798c4640bad75c7c3227db910174e72":"a9a1631bf4996954ebc093957b234589":"00000000000000000000000000000000"

AES-128-CFB128 Decrypt NIST KAT #9
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"00000000000000000000000000000000":"96ab5c2ff612d9dfaae8c31f30c42168":"ff4f8391a6a40ca5b25d23bedd44a597":"00000000000000000000000000000000"

AES-128-CFB128 Decrypt NIST KAT #10
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"00000000000000000000000000000000":"ffffffffffffffff0000000000000000":"f807c3e7985fe0f5a50e2cdb25c5109e":"00000000000000000000000000000000"

AES-128-CFB128
Decrypt NIST KAT #11
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"00000000000000000000000000000000":"ffffffffffffffff8000000000000000":"41f992a856fb278b389a62f5d274d7e9":"00000000000000000000000000000000"

AES-128-CFB128 Decrypt NIST KAT #12
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"00000000000000000000000000000000":"ffffffffffffffffc000000000000000":"10d3ed7a6fe15ab4d91acbc7d0767ab1":"00000000000000000000000000000000"

AES-192-CFB128 Encrypt NIST KAT #1
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"ffffffffffffffffffc000000000000000000000000000000":"00000000000000000000000000000000":"00000000000000000000000000000000":"8dfd999be5d0cfa35732c0ddc88ff5a5"

AES-192-CFB128 Encrypt NIST KAT #2
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"fffffffffffffffffffe000000000000000000000000000000":"00000000000000000000000000000000":"00000000000000000000000000000000":"02647c76a300c3173b841487eb2bae9f"

AES-192-CFB128
Encrypt NIST KAT #3
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"fffffffffffffffffff000000000000000000000000000000":"00000000000000000000000000000000":"00000000000000000000000000000000":"172df8b02f04b53adab028b4e01acd87"

AES-192-CFB128 Encrypt NIST KAT #4
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"d184c36cf0dddfec39e65419500602223787 1a47c33d3198":"00000000000000000000000000000000":"00000000000000000000000000000000":"2e19fb60a3e1de0166f483c97824a978"

AES-192-CFB128 Encrypt NIST KAT #5
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"4c6994ffa9dcdc805b60c2c0095334c42d95a8fc0ca5b080":"00000000000000000000000000000000":"00000000000000000000000000000000":"7656709538dd5fec41e0ce6a0f8e207d"

AES-192-CFB128 Encrypt NIST KAT #6
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"c88f5b00a4ef9a6840e2acaf33f00a3bdc4e25895303fa72":"00000000000000000000000000000000":"00000000000000000000000000000000":"a67cf333b314d411d3c0ae6e1cfcd8f5"

AES-192-CFB128
Encrypt NIST KAT #7
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"000000000000000000000000000000000000000000000000":"9c2d8842e5f48f57648205d39a239af1":"00000000000000000000000000000000":"c9b8135ff1b5adc413dfd053b21bd96d"

AES-192-CFB128 Encrypt NIST KAT #8
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"000000000000000000000000000000000000000000000000":"bff52510095f518ecca60af4205444bb":"00000000000000000000000000000000":"4a3650c3371ce2eb35e389a171427440"

AES-192-CFB128 Encrypt NIST KAT #9
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"00000000000000000000000000000000000000000000000000":"51719783d3185a535bd75adc65071ce1":"00000000000000000000000000000000":"4f354592ff7c8847d2d0870ca9481b7c"

AES-192-CFB128 Encrypt NIST KAT #10
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"00000000000000000000000000000000000000000000000000":"fffffffffffffe000000000000000000":"00000000000000000000000000000000":"f34e4a6324ea4a5c39a661c8fe5ada8f"

AES-192-CFB128
Encrypt NIST KAT #11
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"00000000000000000000000000000000000000000000000000":"ffffffffffffff000000000000000000":"00000000000000000000000000000000":"0882a16f44088d42447a29ac090ec17e"

AES-192-CFB128 Encrypt NIST KAT #12
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"00000000000000000000000000000000000000000000000000":"ffffffffffffff800000000000000000":"00000000000000000000000000000000":"3a3c15bfc11a9537c130687004e136ee"

AES-192-CFB128 Decrypt NIST KAT #1
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"fffffffffffffffffffffffffffffffffffffffffffffe00000":"00000000000000000000000000000000":"60136703374f64e860b48ce31f930716":"00000000000000000000000000000000"

AES-192-CFB128 Decrypt NIST KAT #2
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"fffffffffffffffffffffffffffffffffffffffffffff00000":"00000000000000000000000000000000":"8d63a269b14d506ccc401ab8a9f1b591":"00000000000000000000000000000000"

AES-192-CFB128 Decrypt NIST
KAT #3
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"fffffffffffffffffffffffffffffffffffffffffffff80000":"00000000000000000000000000000000":"d317f81dc6aa454aee4bd4a5a5cff4bd":"00000000000000000000000000000000"

AES-192-CFB128 Decrypt NIST KAT #4
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"98c6b8e01e379fbd14e61af6af891596583565f2a27d59e9":"000000000000000000000000000000000000":"19c80ec4a6deb7e5ed1033dda933498f":"00000000000000000000000000000000"

AES-192-CFB128 Decrypt NIST KAT #5
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"b3ad5cea1dddc214ca969ac35f37dae1a9a9d1528f89bb35":"000000000000000000000000000000000000":"3cf5e1d21a17956d1dffad6a7c41c659":"00000000000000000000000000000000"

AES-192-CFB128 Decrypt NIST KAT #6

depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"45899367c3132849763073c435a9288a766c8b9ec2308516":"00000000000000000000000000000000":"69fd12e8505f8ded2fdcb197a121b362":"00000000000000000000000000000000"

AES-192-CFB128 Decrypt NIST KAT #7
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"000000000000000000000000000000000000000000000000":"1b077a6af4b7f98229de786d7516b639":"275cfc0413d8ccb70513c3859b1d0f72":"00000000000000000000000000000000"

AES-192-CFB128
Decrypt NIST KAT #8
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"000000000000000000000000000000000000000000000000":"9c2d8842e5f48f57648205d39a239af1":"c9b8135ff1b5adc413dfd053b21bd96d":"00000000000000000000000000000000"

AES-192-CFB128 Decrypt NIST KAT #9
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"000000000000000000000000000000000000000000000000":"bff52510095f518ecca60af4205444bb":"4a3650c3371ce2eb35e389a171427440":"00000000000000000000000000000000"

AES-192-CFB128 Decrypt NIST KAT #10
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"000000000000000000000000000000000000000000000000":"ffffffffffffffffffff000000000000":"54d632d03aba0bd0f91877ebdd4d09cb":"00000000000000000000000000000000"

AES-192-CFB128 Decrypt NIST KAT #11
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"000000000000000000000000000000000000000000000000":"ffffffffffffffffffff800000000000":"d3427be7e4d27cd54f5fe37b03cf0897":"00000000000000000000000000000000"

AES-192-CFB128
Decrypt NIST KAT #12
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"000000000000000000000000000000000000000000000000":"ffffffffffffffffffffc00000000000":"b2099795e88cc158fd75ea133d7e7fbe":"00000000000000000000000000000000"

AES-256-CFB128 Encrypt NIST KAT #1
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"fffffffe0000000000000000000000000000000000000000000000000000000000000000":"00000000000000000000000000000000":"00000000000000000000000000000000":"bbd1097a62433f79449fa97d4ee80dbf"

AES-256-CFB128 Encrypt NIST KAT #2
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"fffffff0000000000000000000000000000000000000000000000000000000000000000":"00000000000000000000000000000000":"00000000000000000000000000000000":"07058e408f5b99b0e0f061a1761b5b3b"

AES-256-CFB128 Encrypt NIST KAT #3
depends_on:MBEDTLS_CIPHER_MODE_CFB

aes_encrypt_cfb128:"fffffff800000000000000000000000000000000000000000000000000000000":"000000000000000000000000000000000000":"00000000000000000000000000000000":"5fd1f13fa0f31e37fabde328f894eac2"

AES-256-CFB128
Encrypt NIST KAT #4
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"13428b5e4c005e0636dd338405d173ab135dec2a25c22c5df0722d69dcc43887":"000000000000000000000000000000000000":"00000000000000000000000000000000":"649a71545378c783e368c9ade7114f6c"

AES-256-CFB128 Encrypt NIST KAT #5
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"07eb03a08d291d1b07408bf3512ab40c91097ac77461aad4bb859647f74f00ee":"000000000000000000000000000000000000":"00000000000000000000000000000000":"47cb030da2ab051dfc6c4bf6910d12bb"

AES-256-CFB128 Encrypt NIST KAT #6
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"90143ae20cd78c5d8ebdd6cb9dc1762427a96c78c639bccc41a61424564eafe1":"000000000000000000000000000000000000":"00000000000000000000000000000000":"798c7c005dee432b2c8ea5dfa381ecc3"

AES-256-CFB128
Encrypt NIST KAT #7
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"0000000000000000000000000000000000000000000000000000000000000000":"0b24af36193ce4665f2825d7b4749c98":"00000000000000000000000000000000":"a9ff75bd7cf6613d3731c77c3b6d0c04"

AES-256-CFB128 Encrypt NIST KAT #8
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"0000000000000000000000000000000000000000000000000000000000000000":"761c1fe41a18acf20d241650611d90f1":"00000000000000000000000000000000":"623a52fcea5d443e48d9181ab32c7421"

AES-256-CFB128 Encrypt NIST KAT #9
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"0000000000000000000000000000000000000000000000000000000000000000":"8a560769d605868ad80d819bdba03771":"00000000000000000000000000000000":"38f2c7ae10612415d27ca190d27da8b4"

AES-256-CFB128 Encrypt NIST KAT #10
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"0000000000000000000000000000000000000000000000000000000000000000":"ffffffffffffffffffffffffe0000000":"00000000000000000000000000000000":"2be1fae5048a25582a679ca10905eb80"

AES-256-CFB128
Encrypt NIST KAT #11
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_encrypt_cfb128:"0000000000000000000000000000000000000000000000000000000000000000":"ffffffffffffffffffffffff0000000":"00000000000000000000000000000000":"da86f292c6f41ea34fb2068df75ecc29"

AES-256-CFB128 Encrypt NIST KAT #12
depends_on:MBEDTLS_CIPHER_MODE_CFB

aes_encrypt_cfb128:"00000000000000000000000000000000000000000000000000000000000000000000000000000000":"ffffffffffffffffffffffffffff8000000":"00000000000000000000000000000000":"220df19f85d69b1b562fa69a3c5beca5"

AES-256-CFB128 Decrypt NIST KAT #1
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"fffffffff8000000000000000000000000000000000000000000000000000000000000":"0000000000000000000000000000000000":"be66cfea2fecd6bf0ec7b4352c99bcaa":"00000000000000000000000000000000"

AES-256-CFB128 Decrypt NIST KAT #2
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"fffffffffc0000000000000000000000000000000000000000000000000000000000000":"0000000000000000000000000000000000":"df31144f87a2ef523facdcf21a427804":"00000000000000000000000000000000"

AES-256-CFB128
Decrypt NIST KAT #3
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"fffffffffe0000000000000000000000000000000000000000000000000000000000000":"0000000000000000000000000000000000":"b5bb0f5629fb6aae5e1839a3c3625d63":"00000000000000000000000000000000"

AES-256-CFB128 Decrypt NIST KAT #4
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"1d85a181b54cde51f0e098095b2962fdc93b51fe9b88602b3f54130bf76a5bd9":"0000000000000000000000000000000000":"531c2c38344578b84d50b3c917bbb6e1":"00000000000000000000000000000000"

AES-256-CFB128 Decrypt NIST KAT #5
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"dc0eba1f2232a7879ded34ed8428eeb8769b056bbaf8ad77cb65c3541430b4cf":"0000000000000000000000000000000000":"fc6aec906323480005c58e7e1ab004ad":"00000000000000000000000000000000"

AES-256-CFB128 Decrypt NIST KAT #6
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"f8be9ba615c5a952cabbca24f68f8593039624d524c816acda2c9183bd917cb9":"0000000000000000000000000000000000":"a3944b95ca0b52043584ef02151926a8":"00000000000000000000000000000000"

AES-256-CFB128
Decrypt NIST KAT #7
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"00000000000000000000000000000000000000000000000000000000000000000000000000000000":"761c1fe41a18acf20d241650611d90f1":"623a52fcea5d443e48d9181ab32c7421":"00000000000000000000000000000000"

AES-256-CFB128 Decrypt NIST KAT #8
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"00000000000000000000000000000000000000000000000000000000000000000000000000000000":"8a560769d605868ad80d819bdba03771":"38f2c7ae10612415d27ca190d27da8b4":"00000000000000000000000000000000"

AES-256-CFB128 Decrypt NIST KAT #9
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"00000000000000000000000000000000000000000000000000000000000000000000000000000000":"91fbef2d15

a97816060bee1feaa49afe":"1bc704f1bce135ceb810341b216d7abe":"00000000000000000000000000000000"

AES-256-CFB128 Decrypt NIST KAT #10
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"0000000000000000000000000000000000000000000000000000000000000000":"e0000000000000000000000000000000":"9b80eefb7ebe2d2b16247aa0efc72f5d":"00000000000000000000000000000000"

AES-256-CFB128
Decrypt NIST KAT #11
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"0000000000000000000000000000000000000000000000000000000000000000":"f0000000000000000000000000000000":"7f2c5ece07a98d8bee13c51177395ff7":"00000000000000000000000000000000"

AES-256-CFB128 Decrypt NIST KAT #12
depends_on:MBEDTLS_CIPHER_MODE_CFB
aes_decrypt_cfb128:"0000000000000000000000000000000000000000000000000000000000000000":"f8000000000000000000000000000000":"7818d800dcf6f4be1e0e94f403d1e4c2":"00000000000000000000000000000000"

AES-128-CFB8 Encrypt NIST MMT #0
aes_encrypt_cfb8:"c57d699d89df7cfbef71c080a6b10ac3":"fcb2bc4c006b87483978796a2ae2c42e":"61":"24"

AES-128-CFB8 Encrypt NIST MMT #1
aes_encrypt_cfb8:"0d8f3dc3edee60db658bb97faf46fba3":"e481fdc42e606b96a383c0a1a5520ebb":"aacd":"5066"

AES-128-CFB8
Encrypt NIST MMT #2
aes_encrypt_cfb8:"c8fe9bf77b930f46d2078b8c0e657cd4":"f475c64991b20eaee183a22629e21e22":"c90635":"d27691"

AES-128-CFB8 Encrypt NIST MMT #3
aes_encrypt_cfb8:"280cf81af5cc7e7363579c1da03390e6":"5d6cf4722d0e21f1d9ced53a0e36c342":"b2a22ced":"73f3aebf"

AES-128-CFB8 Encrypt NIST MMT #4
aes_encrypt_cfb8:"5d5e7f20e0a66d3e09e0e5a9912f8a46":"052d7ea0ad1f2956a23b27afe1d87b6b":"b84a90fc6d":"1a9a61c307"

AES-128-CFB8 Encrypt NIST MMT #5
aes_encrypt_cfb8:"ec89fb348787cf902ca973c47081438d":"528fe95c711bd13f37bc52cc9e96d45c":"14253472e99d":"cfc247e33a3b"

AES-128-CFB8 Encrypt NIST MMT #6
aes_encrypt_cfb8:"6607987c354809cba818639dcd185147":"552c101a0b7c0ca143af258453937fa3":"9b1a5a1369166e":"b7ab2a4cc71904"

AES-128-CFB8 Encrypt NIST MMT #7
aes_encrypt_cfb8:"c028e6bf2b749ffa86759f2f84e93cb0":"288c752d9faccf367e5d0cca1fa6ec3b":"324015878cdc82bf":"873250152fc6a5bb"

AES-128-CFB8 Encrypt NIST MMT #8
aes_encrypt_cfb8:"d01da95d2c2a61da06ea78cfba59cc30":"f9a393ad90814faf262e3a5b1d97592e":"57c1a30e48166d9640":"e9a8c3b776edd39e3d"

AES-128-CFB8
Encrypt NIST MMT #9
aes_encrypt_cfb8:"3a6f9159263fa6cef2a075caface5817":"0fc23662b7dbf73827f0c7de321ca36e":"87efeb8d559ed3367728":"8e9c50425614d540ce11"

AES-128-CFB8 Decrypt NIST MMT #0
aes_decrypt_cfb8:"03edfe082550bd5ac8ddf64f42a0547f":"52acd8dab62c981da08e51939cc08dab":"21":"09"

AES-128-CFB8 Decrypt NIST MMT #1
aes_decrypt_cfb8:"38cf776750162edc63c3b5dbe311ab9f":"98fbbd288872c40f1926b16ecaec1561":"4878":"eb24"

AES-128-CFB8 Decrypt NIST MMT #2
aes_decrypt_cfb8:"c9053c87c3e56bc5e52bd31f6545f991":"b8f9640d0923da13fe6eb87b01f0cfa0":"aeb6d2":"910949"

AES-128-CFB8 Decrypt NIST MMT #3
aes_decrypt_cfb8:"e96771f5f20a89ee871261d2d18e1e46":"6e86403e33396655907ae06ef192262f":"83cab2f3":"3b7f1f1c"

AES-128-CFB8 Decrypt NIST MMT #4
aes_decrypt_cfb8:"92ad13ecb60bde1bb3b34ce07867672b":"f95a4060b8f80e3f839d4c3ca33dad94":"49f73e652b":"17b9b9e16d"

AES-128-CFB8 Decrypt NIST MMT #5
aes_decrypt_cfb8:"eb57b8dd076e7bbb33d4bfc4d7ecb27e":"51135997a067dcd2e016c57134c5fa52":"b0eacbf2ca46":"ca989fa4e818"

AES-128-CFB8
Decrypt NIST MMT #6
aes_decrypt_cfb8:"70abc48bb1be490183f0fe3df56195ff":"e251f179174b71ee1e488ab3dd200483":"08fbef9b2a369a":"5405da1186b7e0"

AES-128-CFB8 Decrypt NIST MMT #7
aes_decrypt_cfb8:"1273b8e0eee1a1ca827059b4d0a3a55d":"622cab49092d026f554dd98a6441dc26":"b3cb9d8892423aeb":"d497df73afb9787c"

AES-128-CFB8 Decrypt NIST MMT #8
aes_decrypt_cfb8:"49437e06b6faa5f20fd98bf71f8ff554":"63c818e0d3cb5b7054ef3e1e87df0e12":"01992a986279c3685e":"f203bcd402b65919da"

AES-128-CFB8 Decrypt NIST MMT #9
aes_decrypt_cfb8:"6399c1dc068ba3509845628fa9ed1a96":"1157c2766c86b754df485be9dd5851df":"c9c284e9abbfe6fb11fe":"feff4e2e2458addf2a54"

AES-192-CFB8 Encrypt NIST MMT #0
aes_encrypt_cfb8:"32a1b0e3da368db563d7316b9779d3327e53d9a6d287ed97":"3dd0e7e21f09d5842f3a699da9b57346":"54":"6d"

AES-192-CFB8 Encrypt NIST MMT #1
aes_encrypt_cfb8:"a6381dcc18dd85d7729c1dce90743bbe1df580d857f5b9c4":"c0ac501fad7f4a1465daf32e18fc1a4f":"a456":"8fb6"

AES-192-CFB8
Encrypt NIST MMT #2
aes_encrypt_cfb8:"d08dbee4732c7ffc544c1695b201d30e795037325ef0aa18":"a1e39aeeb972a8d70aa0fc7d6fac6eac":"fd115d":"c4c016"

AES-192-CFB8 Encrypt NIST MMT #3
aes_encrypt_cfb8:"277185a4a440869920f523c4d578fc5bedd33aee8d2ebaf7":"67be00572f82aabc13d6e5a2e51d1f08":"88e07061":"8bb630ba"

AES-192-CFB8 Encrypt NIST MMT #4
aes_encrypt_cfb8:"83f70fdce47306fcbb8c21b6a8b3209f7ec185fef4deebd4":"ff73b310cf7e62ce6f501092fa6cc888":"36664e222d":"20855555d1"

AES-192-CFB8 Encrypt NIST MMT #5
aes_encrypt_cfb8:"c5be271a29f4a29e085e8e98196601dcb88ccc03e559a304":"9f51fa2eb8a084718f7240e47d135dce":"b57f12342a62":"73ff9bf3ec4b"

AES-192-CFB8 Encrypt NIST MMT #6
aes_encrypt_cfb8:"9c55322e6d495be01076d4b80371ad1479ae5636ff9861f5":"2b79cfc1ff37254dedf5924a6b61e3e0":"6dcede43c2ee65":"7c897658282220"

AES-192-CFB8 Encrypt NIST MMT #7
aes_encrypt_cfb8:"6e78ccece7d1b2a3c08cf0de738bee33cbbbf78d9bf4922c":"4bbe15b1e94a7b97250a2136d8804e46":"ceda42527871f802":"d92ff89045b1917f"

AES-192-CFB8
Encrypt NIST MMT #8
aes_encrypt_cfb8:"13c98665746f7825b37b404916240adbd1e4364be1d05c63":"0e479fbd5f3961f38b8a26be1f2d65c5":"1b0a63d73464ab3c8a":"5485847e5d3c2e2cc4"

AES-192-CFB8 Encrypt NIST MMT #9
aes_encrypt_cfb8:"537e7bf661fd4024a024613f15b13690f7d0c847c1e18965":"3a81f9d9d3c155b0caad5d73349476fc":"d3d8b9b984adc24237ee":"3879fea72ac99929e53a"

AES-192-CFB8 Decrypt NIST MMT #0
aes_decrypt_cfb8:"7dbdc15ad4034ed828dc862799b7adc9abd68eaf9d526d5d":"4359683af5a3a85c248fb7f5506f317b":"25":"2d"

AES-192-CFB8 Decrypt NIST MMT #1

aes_decrypt_cfb8:"3a2cdf9c9608c1dd6233d03dd855293b0885915114b25279":"e7a28ee34acc52128ddae658ec6398a2":"0678":"7b04"

AES-192-CFB8 Decrypt NIST MMT #2
aes_decrypt_cfb8:"c984b99a6cc5bc88003143cbe4b755e6e30ba94114f7ad1e":"41e3b8fd138f8c358dfeef420302f634":"037cf6":"658d0a"

AES-192-CFB8 Decrypt NIST MMT #3
aes_decrypt_cfb8:"39747da225bdc0c53c3463fd686dbe19d14157535171f91d":"77d3a5ad8bbdb169f8d29e5f21798651":"0fb0cee2":"2d191f2f"

AES-192-CFB8 Decrypt NIST MMT
#4
aes_decrypt_cfb8:"4cd13179dfa16d01c6a8633dfc8783e723e72114c9b0d50a":"6657c46c99d642474c330d8016b71dbe":"09d914cf0b":"105a64c872"

AES-192-CFB8 Decrypt NIST MMT #5
aes_decrypt_cfb8:"5dcc9b8d8a456e9917cd8d54d7f7100b34964b4ed2d398a0":"4fa295a8987f1b010ce4e011fbf94156":"288c752d9fac":"98f332d37b78"

AES-192-CFB8 Decrypt NIST MMT #6
aes_decrypt_cfb8:"c8baf0204ef80b8e0125efe43a0bccdfd0f356b62e6c75fe":"e9144bf2cbc5720a1b4cb6f37d11edff":"c9981a34b7aa89":"56bb4c3cae53b3"

AES-192-CFB8 Decrypt NIST MMT #7
aes_decrypt_cfb8:"64e40763f38a63ae378c32052b0ae3aa538bb868a04ac985":"aacf65089e4b285438451ffdcd0f6389":"d8fcf83a88510a0d":"b567411bc61b0a76"

AES-192-CFB8 Decrypt NIST MMT #8
aes_decrypt_cfb8:"7bfdca9605f17253f203efffc92da96fde023007d22cdad0":"45c09e44036070f8a7737a5176b8cf26":"9c195b1944c4af5bfb":"89358df65c3ef14d26"

AES-192-CFB8 Decrypt NIST MMT #9
aes_decrypt_cfb8:"baf08b76317a65c5f07ae6f57eb0e65488659324d29709e3":"0a02846b62abb693ef31d754842eed29":"729c0b6deb75fa6eb5e8":"9895932402393dc33a60"

AES-256-CFB8
Encrypt NIST MMT #0
aes_encrypt_cfb8:"34e8091cee09f1bd3ebf1e8f05f51bfbd4899ef2ae006a3a0f7875052cdd46c8":"43eb4dcc4b04a80216a20e4a09a7abb5":"f9":"28"

AES-256-CFB8 Encrypt NIST MMT #1
aes_encrypt_cfb8:"e04e43173113109e1343393842fe6caef3f8a2e506d7f55f83dcb10444c6ad23":"a38b88a293b077fb5546636aad90d663":"2914":"69a6"

AES-256-CFB8 Encrypt NIST MMT #2
aes_encrypt_cfb8:"064874092f7a13cc4462247ad423d0e96edf42e8b67a5a23b7a0a6477b098e66":"338c552ff1eca14408e05d8cf9f3b31b":"b974fa":"1cff95"

AES-256-CFB8 Encrypt NIST MMT #3
aes_encrypt_cfb8:"56794adb0ef04aeddeabd650de736531d408837954b919002c33edfdff976cc2":"71b5526facea4236d33f1f4107e4b04f":"db774912":"f04d9d4f"

AES-256-CFB8 Encrypt NIST MMT #4
aes_encrypt_cfb8:"dddd7f234e7d0e6ec64560b96430986a856f2ee9805443a7946e31601ef6679d":"e20f39db0025eb24491bd06012887108":"ad1d5311ea":"19cc97a662"

AES-256-CFB8 Encrypt NIST MMT #5
aes_encrypt_cfb8:"ec73a760272c83f91771b3ab7b188715c6d6afb9c554feae83856e966a3863d0":"ae7bfa38fd25778fcf66ce8157f6e42e":"02fe724fbc5d":"b0eca63405f4"

AES-256-CFB8
Encrypt NIST MMT #6
aes_encrypt_cfb8:"a66874ca0b70fb98b37c033ec96413f339adae02acade015b9f016b459db3309":"6ed480d9e4ed031cf66bb1e07f8d5514":"b4777e6bcd9a05":"8c017397ad5bab"

AES-256-CFB8 Encrypt NIST MMT #7
aes_encrypt_cfb8:"a3dbbb775ada92b0b8ed1632444e21c1c86ff3eba8f628307306e766b8c15b5c":"4ec56a8e541f5cfe7b8ab947bfa4fd08":"1d70a5a82badf5ea":"1e22bebebeacd81d"

AES-256-CFB8 Encrypt NIST MMT #8
aes_encrypt_cfb8:"64135e67c0ca1acef3360d930afcd726c5b04861a69c1b6a48bde1daf20f3b1f":"5377a154d5f948189f9aa57b466c16b2":"a36ca5ea382a322eef":"3105016567d3174aed"

AES-256-CFB8 Encrypt NIST MMT #9
aes_encrypt_cfb8:"ebbb4566b5e182e0f072466b0b311df38f9175bc0213a5530bce2ec4d74f400d":"0956a48e01002c9e16376d6e308dbad1":"b0fe25ac8d3d28a2f471":"638c6823e7256fb5626e"

AES-256-CFB8 Decrypt NIST MMT #0
aes_decrypt_cfb8:"1687831580cb764321a9d674dbd0a9640f668b0f58ef01b87a710b3095d5f855":"6cd5bec6d6e1fd23afc543b8f80d3f89":"6f":"98"

AES-256-CFB8 Decrypt
NIST MMT #1
aes_decrypt_cfb8:"b6b504e8b7065373ea31cd549e52eda7cb96fd1db14eddacbc420085ab48b747":"870ecd45b1241803ddaf8bad15a025d7":"17d4":"3572"

AES-256-CFB8 Decrypt NIST MMT #2
aes_decrypt_cfb8:"6ad3105e15fb5b742bf4fe1eb8e98c6c1ffea653107c84f6b42ed1232a0bbc21":"17534c89c4eae5dea6ea353dde7b1623":"a9841e":"f9411a"

AES-256-CFB8 Decrypt NIST MMT #3
aes_decrypt_cfb8:"758f3fa8b2b289f19fd59e7316be40b904eff7f565caac4570f972360e0da787":"b21335ae980898fa92c4b3069e532973":"84b35e25":"47887872"

AES-256-CFB8 Decrypt NIST MMT #4

aes_decrypt_cfb8:"802e854eb799500975d960a67885820d195e02ab23d51f15e5cdbcee86a1580c":"94478c4e44e2fa8d2e6bc43d384597e6":"d1e96bf1e8":"ed414b5689"

AES-256-CFB8 Decrypt NIST MMT #5
aes_decrypt_cfb8:"3a0c03ca9d1e5d49bb37f9041f88d159c3f1d5ce26c798f59ed54a93f0a0e600":"9aae38ba832e4b093b50444074517d20":"74410ccd12da":"8207eee2a7ab"

AES-256-CFB8 Decrypt NIST MMT #6
aes_decrypt_cfb8:"ee05462128fea75e919f6f436cb198f222847d698a283f5767df682d33d3ce77":"d2ad55e41887075184635112a22fc093":"ff039e89877b44":"aff3aa4c24e353"

AES-256-CFB8
Decrypt NIST MMT #7
aes_decrypt_cfb8:"08abbdcc3eb9c1717db1faa38dcd0893afd5e16e2596747af58f8d61ebedf9cd":"b925c8dc9a9b55a4372ea6d37d21c1eb":"e176ba99ea602fd9":"b7370050288bf600"

AES-256-CFB8 Decrypt NIST MMT #8
aes_decrypt_cfb8:"56d404a893fb3b3f594aab18939230b096646a37a781629fbd9270f3891a5cea":"e5906b36f2d97e6f2db19b6c7a3ce319":"c55a9a917a809a784b":"e44995bbb0fff40fee"

AES-256-CFB8 Decrypt NIST MMT #9
aes_decrypt_cfb8:"ec13062551e4d7291e320f565b749eea1809b663b26f2c4d53b52058b833e0ad":"fbfa5a528e20863012790c2abafb5a0c":"2bfc3f0209307140101a":"547bfd642cf6e12ed942"

```
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
   <Configuration>Release</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\pkey\pk_verify.c" />
 </ItemGroup>
 <ItemGroup>
```

```
  <ProjectReference Include="mbedTLS.vcxproj">

    <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid>{C429B336-1B30-119C-3B34-21A186D6744F}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>pk_verify</RootNamespace>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
    <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
/>
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
```

```
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
    <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
   <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <LinkIncremental>false</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
   <LinkIncremental>false</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <ClCompile>
     <PrecompiledHeader>
     </PrecompiledHeader>
     <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
      <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
     <SubSystem>Console</SubSystem>
     <GenerateDebugInformation>true</GenerateDebugInformation>
     <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
     <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
   </Link>
   <ProjectReference>
     <LinkLibraryDependencies>false</LinkLibraryDependencies>
   </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
   <ClCompile>
     <PrecompiledHeader>
```

```
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
  </Link>
 </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
```

```
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
 <Import
 Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDkwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTAwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAR6jlGKbJd5
hiDxN789gkOcwpyHI9wRwCrADAOwOkMePBPRlwGdm7mw7Z/EAmu26zRm/hcyrs4M
qk2LabDjPI9Xo4GJMIGGMB0GA1UdDgQWBBQtxZSLJAkEz+2RKMQexM6EtsfgcjBX
BgNVHSMEUDBOgBT6gyXHzPIPYc1Vr1aGiLLeMh4HpqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA4ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgP7S8vFstfUBdNe6ym5GYG5Q+aBVEKqRs
fVW7HNUktSYCIQDo6Jua6o/DJbrpq4qYWq5gv4yGyzPTN+3IaKrEICdaaw==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDgwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDkwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAR7ZB16+t6E
sfahGyKUGJW5mezkzjdaYvc4lbJaKNRwFRfc3F/fmNOSsUFSg/F0N+vUE+doKiPC
8wRwLzvm4s+5o4GJMIGGMB0GA1UdDgQWBBT6gyXHzPIPYc1Vr1aGiLLeMh4HpjBX
BgNVHSMEUDBOgBS40mLt93U8Sh8ZGiDVAhRSiBPcXqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA3ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgO4el1ZPhlIli/qNR2SIEiuvs5Mmy868i
N2Rv5X/VxIECIA/8rUALQxW38XSdBVX3e/jzu7ju47n1YwEqD9K9WdVv
-----END
 CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDcwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDgwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAARpQeQ/YGQj
```

nl7Szo6WStJ1u7xunTL5jBkXH8aAVSm0qiX4AD/7YPxa5EnGzZdLTn25vQVnfQAG
pMx8P1lYiGYCo4GJMIGGMB0GA1UdDgQWBBS40mLt93U8Sh8ZGiDVAhRSiBPcXjBX
BgNVHSMEUDBOgBREq5J3toJPxZ3O+ssJ5vkkU0RJE6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA2ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhANwGf+F4a+kmXWz8UjSpRkaToTV6EFWw
/Tjzj0tQhDoAAiEA19RxeWOVBBpM6LOHg6v5Lf54YN1snkLf+sEXyZCuWQQ=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDYwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDcwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASNOj4d4MEA
7p/3miijqG4ToE4opKPAm+3BTIGrJTYT14++TSiUICl0ASXj+xeUcLMIaXTN042s
LsHxpShzQaL0o4GJMIGGMB0GA1UdDgQWBBREq5J3toJPxZ3O+ssJ5vkkU0RJEzBX
BgNVHSMEUDBOgBSjovYaC/m6Li9Tp0V9iZRs9267Q6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA1ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAKGcf+c442c/XiwubbaiQvsoZ7EoVxuM
oKmia0gPyBNkAiEA83asjJ5FDXQuLyZpczviXrbmqgCPOfYadtvkc0cxMis=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDUwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDYwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASA9qWoAUHr
nn+3kxyNrjPJk82WDLimW21RN51uxpobadv8YgGEDRdP+Ok+uRqQSUsA6ZXfF3iG
r2GjfQ3wMDH8o4GJMIGGMB0GA1UdDgQWBBSjovYaC/m6Li9Tp0V9iZRs9267QzBX
BgNVHSMEUDBOgBTXh06MAV9S4l4lG1TKOrKRBh4qn6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA0ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgcjZNFWJtlDmoPZbAxqsGczRYK0lfPgu6
g1H7pp0ce+wCIDj9BRZM2OB9EF0e+MDKGjyZGfvfrL6Ir47x/KrM6H8T
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDQwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDUwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQEdT0OFf5G
UcrgX2XllCyJzP94NZ464GsgB6psNLsDeL+j7AU+oJy7VLvW/lHh3ODgl08Z9bhq
LFBmNjnHbm8Qo4GJMIGGMB0GA1UdDgQWBBTXh06MAV9S4l4lG1TKOrKRBh4qnzBX
BgNVHSMEUDBOgBQox4F1NsZunlsduoGvzIgRSYfB36EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAzggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAIW++zqDZlLLUk/emePohdNOp5JO3wS9
XvkBJ6Wua7GBAiAdx+EKmdjVrwnzrQltTgnmSfGMXhKNYifK3uD83W3pcQ==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G

A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDMwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDQwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQUXDgcUVNT
9hovbZE5HL6rjOb7C55wEuWKThV/CcZ4rWrXx7VXHYdD/R3aDA7JSvYpm2sTok4i
sblDzhZM/GDNo4GJMIGGMB0GA1UdDgQWBBQox4F1NsZunlsduoGvzIgRSYfB3zBX
BgNVHSMEUDBOgBQApzZdtBdD3dLxouQpr/aDiVttd6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAyggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgAkiNhqFAZXSUWEDK91OZvQGdeZOtd6mC
+Wv3fGk3t28CIEKOwidkUTUaiPdZ4efmAr+CEeGzdq27ob2S+nqqHqgV
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDIwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDMwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQRDXDNIi1p
ereudhqwa2LslXgsxnB63Hu5y5lg+1WPruIYPzD/Ho0APveVdzFLVji19+bE4+tF
PYL1SpsN1WfWo4GJMIGGMB0GA1UdDgQWBBQApzZdtBdD3dLxouQpr/aDiVttdzBX
BgNVHSMEUDBOgBT5RCgQ0AlZTQbfFB2+6+w0XRvydaEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAxggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAOnd+7bAofkHVa4KFNjv3TCegw1lrhuM
8Of8wgvrTEGoAiEAsS8iKMpSfXH4D0egg4gLamE6akde965rDtySU+ve9lg=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDEwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDIwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQWHpv1i6lf
wvNPOP5ka6S0n55EvzoaYK6pbTXP6yMOW/4XZSPKx5Zoq4FMe0cKzGIIFL1rzj1V
2czYB+qvLhyio4GJMIGGMB0GA1UdDgQWBBT5RCgQ0AlZTQbfFB2+6+w0XRvydTBX
BgNVHSMEUDBOgBSh3uHkX5nj86yFEFwjscSWM40P+qEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAI7unGW/gr9tOc3i+dF5N815srgh+FrX
oj9Et74EcSpTAiBubv+vOH0DE0gmYI11HeAIgutWqqMIC72dZlwTF/Vi3g==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB3jCCAYWgAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDAwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQznn9zHHwL
GO8VR4W9V7vMlxCdoojzEOiX5Y6JtPtFOz866ueHY6zoN0/mJ6DnqnSXilJIUUeW
6eGfqmka7nxko4GRMIGOMB0GA1UdDgQWBBSh3uHkX5nj86yFEFwjscSWM40P+jBf
BgNVHSMEWDBWgBQlFYvU5WboI4fcdPoiQs8/fPHZraEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggkA/KCWhcqToHAw
DAYDVR0TBAUwAwEB/zAKBggqhkjOPQQDAgNHADBEAiBasbuinP+pJTU4oDCVD8zQ
1rJBDSOKIEyWu84/D6Hj6wIgVMPUoO01bPhzllAa/gW8Xk/daey09SBgN3AT9pWU
TDA=

-----END CERTIFICATE-----
-----BEGIN
CERTIFICATE-----
MIIBpTCCAUugAwIBAgIJAPygloXKk6BwMAoGCCqGSM49BAMCMC8xCzAJBgNVBAYT
AlVLMREwDwYDVQQKDAhtYmVkIFRMUzENMAsGA1UEAwwEQ0EwMDAeFw0xNzA2MjIx
MTUwMzJaFw0yNzA2MjMxMTUwMzJaMC8xCzAJBgNVBAYTAlVLMREwDwYDVQQKDAht
YmVkIFRMUzENMAsGA1UEAwwEQ0EwMDBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IA
BFW41/qAwAPpy+Txdc7PKmzZsq9CPiujKU4vpF1ekXnGx2HP420QobwBVVWhkzRm
LwdboH2j65dcCKjQ7mv/dxKjUDBOMB0GA1UdDgQWBBQlFYvU5WboI4fcdPoiQs8/
fPHZrTAfBgNVHSMEGDAWgBQlFYvU5WboI4fcdPoiQs8/fPHZrTAMBgNVHRMEBTAD
AQH/MAoGCCqGSM49BAMCA0gAMEUCIQC7iRcVzwMyfVK5imirJ7MqJQ04euH4CLOt
IZ+SNfaERAIgSU0MWFDosVEIpg8YMqIHeF7Mg4ZyH6+fGazJgVLttUY=
-----END CERTIFICATE-----
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
   <Configuration>Release</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\pkey\key_app.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">

 <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid>{10AE376F-1A70-0297-0216-1FD01AD15D19}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>key_app</RootNamespace>
 </PropertyGroup>

```
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
   <UseDebugLibraries>true</UseDebugLibraries>
   <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
   <UseDebugLibraries>true</UseDebugLibraries>
   <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
    <ConfigurationType>Application</ConfigurationType>
   <UseDebugLibraries>false</UseDebugLibraries>
   <WholeProgramOptimization>true</WholeProgramOptimization>
   <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
   <UseDebugLibraries>false</UseDebugLibraries>
   <WholeProgramOptimization>true</WholeProgramOptimization>
   <CharacterSet>Unicode</CharacterSet>
   <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
 />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
    <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
```

```
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
     <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
 <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
```

<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
<AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
</Link>
<ProjectReference>
<LinkLibraryDependencies>false</LinkLibraryDependencies>
</ProjectReference>
</ItemDefinitionGroup>
<ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
<ClCompile>
<WarningLevel>Level3</WarningLevel>
<PrecompiledHeader>
</PrecompiledHeader>
<Optimization>MaxSpeed</Optimization>
<FunctionLevelLinking>true</FunctionLevelLinking>
<IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
<AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
</ClCompile>
<Link>
<SubSystem>Console</SubSystem>
<GenerateDebugInformation>true</GenerateDebugInformation>
<EnableCOMDATFolding>true</EnableCOMDATFolding>
<OptimizeReferences>true</OptimizeReferences>
<AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
</Link>
</ItemDefinitionGroup>
<ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
<ClCompile>
<WarningLevel>Level3</WarningLevel>
<PrecompiledHeader>
</PrecompiledHeader>
<Optimization>MaxSpeed</Optimization>
<FunctionLevelLinking>true</FunctionLevelLinking>
<IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
<AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
</ClCompile>
<Link>
<SubSystem>Console</SubSystem>
<GenerateDebugInformation>true</GenerateDebugInformation>
<EnableCOMDATFolding>true</EnableCOMDATFolding>
<OptimizeReferences>true</OptimizeReferences>
<AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>

```
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.targets"
 />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,A8A95B05D5B7206B

9Qd9GeArejl1GDVh2lLV1bHt0cPtfbh5h/5zVpAVaFpqtSPMrElp50Rntn9et+JA
7VOyboR+Iy2t/HU4WvA687k3Bppe9GwKHjHhtl//8xFKwZr3Xb5yO5JUP8AUctQq
Nb8CLlZyuUC+52REAAthdWgsX+7dJO4yabzUcQ22Tp9JSD0hiL43BlkWYUNK3dAo
PZlmiptjnzVTjg1MxsBSydZinWOLBV8/JQgxSPo2yD4uEfig28qbvQ2wNIn0pnAb
GxnSAOazkongEGfvcjIIs+LZN9gXFhxcOh6kc4Q/c99B7QWETwLLkYgZ+z1a9VY9
gEU7CwCxYCD+h9hY6FPmsK0/lC4O7aeRKpYq00rPPxs6i7phiexg6ax6yTMmArQq
QmK3TAsJm8V/J5AWpLEV6jAFgRGymGGHnof0DXzVWZidrcZJWTNuGEX90nB3ee2w
PXJEFWKoD3K3aFcSLdHYr3mLGxP7H9ThQai9VsycxZKS5kwvBKQ//YMrmFfwPk8x
vTeY4KZMaUrveEel5tWZC94RSMKgxR6cyE1nBXyTQnDOGbfpNNgBKxyKbINWoOJU
WJZAwlsQn+QzCDwpri7+sV1mS3gBE6UY7aQmnmiiaC2V3Hbphxct/en5QsfDOt1X
JczSfpRWLlbPznZg8OQh/VgCMA58N5DjOzTIK7sJJ5r+94ZBTCpgAMbF588f0NTR
KCe4yrxGJR7X02M4nvD4IwOlpsQ8xQxZtOSgXv4LkxvdU9XJJKWZ/XNKJeWztxSe
Z1vdTc2YfsDBA2SEv33vxHx2g1vqtw8SjDRT2RaQSS0QuSaMJimdOX6mTOCBKk1J
9Q5mXTrER+/LnK0jEmXsBXWA5bqqVZIyahXSx4VYZ7l7w/PHiUDtDgyRhMMKi4n2
iQvQcWSQTjrpnlJbca1/DkpRt3YwrvJwdqb8asZU2VrNETh5x0QVefDRLFiVpif/
tUaeAe/P1F8OkS7OIZDs1SUbv/sD2vMbhNkUoCms3/PvNtdnvgL4F0zhaDpKCmlT
P8vx49E7v5CyRNmED9zZg4o3wmMqrQO93PtTug3Eu9oVx1zPQM1NVMyBa2+f29DL
1nuTCeXdo9+ni45xx+jAI4DCwrRdhJ9uzZyC6962H37H6D+5naNvClFR1s6li1Gb
nqPoiy/OBsEx9CaDGcqQBp5Wme/3XW+6z1ISOx+igwNTVCT14mHdBMbya0eIKft5
X+GnwtgEMyCYyyWuUct8g4RzErcY9+yW9Om5Hzpx4zOuW4NPZgPDTgK+t2RSL/Yq
rE1njrgeGYcVeG3f+OftH4s6fPbq7t1A5ZgUscbLMBqr9tK+OqygR4EgKBPsH6Cz
L6zlv/2RV0qAHvVuDJcIDIgwY5rJtINEm32rhOeFNJwZS5MNIC1czXZx5//ugX7l
I4sy5nbVhwSjtAk8Xg5dZbdTZ6mIrb7xqH+fdakZor1khG7bC2uIwibD3cSl2XkR
wN48lslbHnqqagr6Xm1nNOSVl8C/6kbJEsMpLhAezfRtGwvOucoaE+WbeUNolGde
P/eQiddSf0brnpiLJRh7qZrl9XuqYdpUqnoEdMAfotDOID8OtV7gt8a48ad8VPW2
-----END
 RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDMwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDQwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQUXDgcUVNT
9hovbZE5HL6rjOb7C55wEuWKThV/CcZ4rWrXx7VXHYdD/R3aDA7JSvYpm2sTok4i
sblDzhZM/GDNo4GJMIGGMB0GA1UdDgQWBBQox4F1NsZunlsduoGvzIgRSYfB3zBX
BgNVHSMEUDBOgBQApzZdtBdD3dLxouQpr/aDiVttd6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAyggEBMAwGA1UdEwQF
```

MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgAkiNhqFAZXSUWEDK91OZvQGdeZOtd6mC
+Wv3fGk3t28CIEKOwidkUTUaiPdZ4efmAr+CEeGzdq27ob2S+nqqHqgV
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDEwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDIwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQWHpv1i6lf
wvNPOP5ka6S0n55EvzoaYK6pbTXP6yMOW/4XZSPKx5Zoq4FMe0cKzGIIFL1rzj1V
2czYB+qvLhyio4GJMIGGMB0GA1UdDgQWBBT5RCgQ0AlZTQbfFB2+6+w0XRvydTBX
BgNVHSMEUDBOgBSh3uHkX5nj86yFEFwjscSWM40P+qEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAI7unGW/gr9tOc3i+dF5N815srgh+FrX
oj9Et74EcSpTAiBubv+vOH0DE0gmYI11HeAIgutWqqMIC72dZlwTF/Vi3g==
-----END CERTIFICATE-----
[cli-rsa]
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid:always,issuer:always
basicConstraints = CA:false
00
*H
0GXqPMn3@)!A$J.4'ylm|@jaI`OG!pzS]`T(opFr];/>
-----BEGIN CERTIFICATE REQUEST-----
MIICgTCCAWkCAQAwPDELMAkGA1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NMMRow
GAYDVQQDExFQb2xhclNTTCBTZXJ2ZXIgMTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAKkCHz1AatVVU4v9Nu6CZS4VYV6Jv7joRZDb7ogWUtPxQ1BHlhJZ
ZIdr/SvgRvlzvt3PkuGRW+1moG+JKXlFgNCDatVBQ3dfOXwJBEeCsFc5cO2j7BUZ
HqgzCEfBBUKp/UzDtN/dBh9NEFFAZ3MTD0D4bYElXwqxU8YwfhU5rPla7n+SnqYF
W+cTl4W1I5LZ1CQG1QkliXUH3aYajz8JGb6tZSxk65Wb3P5BXhem2mxbacwCuhQs
FiScStzN0PdSZ3PxLaAj/X70McotcMqJCwTbLqZPcG6ezr1YieJTWZ5uWpJl4og/
DJQZo93l6J2VE+0p26twEtxaymsXq1KCVLECAwEAAaAAMA0GCSqGSIb3DQEBBAUA
A4IBAQAQx+EjsPUUYac3t1v24lPOYqrKM52XYDwSnwW5Okjn+YxJowZyd8gfzmfp
vp4+//h5P3VlQDwaXeMTgKCizjf+jdACNJe60/RxYpYFKrvy67ZSr/h7fhdm52Jz
/tSCbh6FwH1075loBuWLuzD7Pvm1X1FJmbp2ceaJozDnXTAKFdVTqdiRYwyg4iPl
krhONGNe132aYZtFssdjSCim+bB+/sagR3SuJPoQ+8EjDXYG75n4ZVa4dAcjVoYk
pg0YK5cuH1FHCXOBO4N1+G0skL8AZwlv+rhKQk6lpGt+AQ8LSjCz2zHUnfpaXXWp
s1dq9ufjbJdaHDjkBY1gZ3BMmXPw
-----END CERTIFICATE REQUEST-----
-----BEGIN CERTIFICATE-----
MIIDITCCAgkCDFOitscEzU2OvIALwTANBgkqhkiG9w0BAQsFADBQMRwwGgYDVQQD
ExNQb2xhclNTTCBUZXN0IENBIHYxMRAwDgYDVQQLEwd0ZXN0aW5nMREwDwYDVQQK
EwhQb2xhclNTTDELMAkGA1UEBhMCTkwwIhgPMjAxNDA2MTkxMDA5MTFaGA8yMDI0
MDYxODEwMDkxMVowTjEaMBgGA1UEAxMRc2VydmVyMS9pbnQtY2EtdjExEDAOBgNV
BAsTB3Rlc3RpbmcxETAPBgNVBAoTCFBvbGFyU1NMMQswCQYDVQQGEwJOTDCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKkCHz1AatVVU4v9Nu6CZS4VYV6J
v7joRZDb7ogWUtPxQ1BHlhJZZIdr/SvgRvlzvt3PkuGRW+1moG+JKXlFgNCDatVB
Q3dfOXwJBEeCsFc5cO2j7BUZHqgzCEfBBUKp/UzDtN/dBh9NEFFAZ3MTD0D4bYEl
XwqxU8YwfhU5rPla7n+SnqYFW+cTl4W1I5LZ1CQG1QkliXUH3aYajz8JGb6tZSxk

65Wb3P5BXhem2mxbacwCuhQsFiScStzN0PdSZ3PxLaAj/X70McotcMqJCwTbLqZP
cG6ezr1YieJTWZ5uWpJl4og/DJQZo93l6J2VE+0p26twEtxaymsXq1KCVLECAwEA
ATANBgkqhkiG9w0BAQsFAAOCAQEAPJl3fbVeTJ6gVAvCoLYM8JY5U7ZhrCCdBghw
WuZBS/TWwf4WLP0G/ZtTyTOENcT0gWHf0/VnXtNPw2/yBjWsLtTXxN2XQlEVf3j/
WcQxWgSESYdx/sT/uTW6qihuONPWkTQizmx7OG6vBuGx3g54s9/oeJKXOraNqud3
G4KBrytOazliMfoKO2hnzaeydpaDtb2tZX8apN/6KqQpTAcXsWrZRW9XEHWq2sNz
IR1nIE1F/9gnqi9Xy0HQprteLRUvM4tEQ35m4H20eS5Y9gJlE/DqXmMQ7aiU8DgP
krj+Z18pcrssO+Etv0BOiPjmU9TWWpDMj34ef7U/OH5qJxkSrA==
-----END
 CERTIFICATE-----
option(INSTALL_MBEDTLS_HEADERS "Install mbed TLS headers." ON)

if(INSTALL_MBEDTLS_HEADERS)

  file(GLOB headers "mbedtls/*.h")

  install(FILES ${headers}
    DESTINATION include/mbedtls
    PERMISSIONS OWNER_READ OWNER_WRITE GROUP_READ WORLD_READ)

endif(INSTALL_MBEDTLS_HEADERS)
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
   <Configuration>Release</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\pkey\ecdh_curve25519.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">

```
    <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid>{82EE497E-12CC-7C5B-A072-665678ACB43E}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>ecdh_curve25519</RootNamespace>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')"
 Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
```

```
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup
 Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
   <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <LinkIncremental>false</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
   <LinkIncremental>false</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <ClCompile>
     <PrecompiledHeader>
     </PrecompiledHeader>
     <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
     <SubSystem>Console</SubSystem>
     <GenerateDebugInformation>true</GenerateDebugInformation>
     <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
     <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
   </Link>
   <ProjectReference>
     <LinkLibraryDependencies>false</LinkLibraryDependencies>
   </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
   <ClCompile>
     <PrecompiledHeader>
     </PrecompiledHeader>
```

```
    <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
     <SubSystem>Console</SubSystem>
     <GenerateDebugInformation>true</GenerateDebugInformation>
     <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
     <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
   </Link>
   <ProjectReference>
     <LinkLibraryDependencies>false</LinkLibraryDependencies>
   </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <ClCompile>
     <WarningLevel>Level3</WarningLevel>
      <PrecompiledHeader>
     </PrecompiledHeader>
     <Optimization>MaxSpeed</Optimization>
     <FunctionLevelLinking>true</FunctionLevelLinking>
     <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
   <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
     <SubSystem>Console</SubSystem>
     <GenerateDebugInformation>true</GenerateDebugInformation>
     <EnableCOMDATFolding>true</EnableCOMDATFolding>
     <OptimizeReferences>true</OptimizeReferences>
     <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
   </Link>

 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
   <ClCompile>
     <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
     </PrecompiledHeader>
     <Optimization>MaxSpeed</Optimization>
     <FunctionLevelLinking>true</FunctionLevelLinking>
```

```
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
   <SubSystem>Console</SubSystem>
   <GenerateDebugInformation>true</GenerateDebugInformation>
   <EnableCOMDATFolding>true</EnableCOMDATFolding>
   <OptimizeReferences>true</OptimizeReferences>
   <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
   <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
  <Import Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
-----BEGIN CERTIFICATE-----
MIIDTzCCAjegAwIBAgIBATANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTEwMjEyMTQ0NDA2WhcNMjEwMjEyMTQ0NDA2WjA8MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxGjAYBgNVBAMTEVBvbGFyU1NMIFNlcnZlciAxMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqQIfPUBq1VVTi/027oJlLhVhXom/
uOhFkNvuiBZS0/FDUEeWEllkh2v9K+BG+XO+3c+S4ZFb7Wagb4kpeUWA0INq1UFD
d185fAkER4KwVzlw7aPsFRkeqDMIR8EFQqn9TMO0390GH00QUUBncxMPQPhtgSVf
CrFTxjB+FTms+Vruf5KepgVb5xOXhbUjktnUJAbVCSWJdQfdphqPPwkZvq1lLGTr
lZvc/kFeF6babFtpzAK6FCwWJJxK3M3Q91Jnc/EtoCP9fvQxyi1wyokLBNsupk9w
bp7OvViJ4lNZnm5akmXiiD8MlBmj3eXonZUT7Snbq3AS3FrKaxerUoJUsQIDAQAB
o10wWzAJBgNVHRMEAjAAMB0GA1UdDgQWBBQfdNY/KcF0dEU7BRIsPai9Q1kCpjAf
BgNVHSMEGDAWgBS0WuSls97SUva51aaVD+s+vMf9/zAOBgNVHQ8BAf8EBAMCAeAw
DQYJKoZIhvcNAQEFBQADggEBABKC/1x0m57EY4H412ue3ghCWgg07VcRKamnUSTs
tnqI5T0mSvuPrxhINdQB6360ibctBkXP3S9rxGHiUdeK/JqxYs2YamCs50TSWpon
p4Hzcmjsw1YgXsQ6pmYwkzU03zqs361gt7JSOzL2dN0IjwIy47qfLQb/AXhX2Ims
7gBuqVpYqJuSHR0qsN/c6WgIE3IrbK1MB6CJTkxBfcSc5E4oUIBHmww+RSVLOczM
nGk3U13dmfG0ndhMtrMyyxBZZSUwoZLjRZ6J5mHSv+k8oo1PYQeiivNEP53mgVaY
ha0gLUIk6zNBRpY1uUmxQ+RQSMIyYPBb1RedHn2s8El2mlo=
-----END
 CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIICLTCCAbKgAwIBAgIBLTAKBggqhkjOPQQDAjA+MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EwHhcN
MTQwNDA5MDg0ODM1WhcNMjQwNDA2MDg0ODM1WjA0MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxEjAQBgNVBAMTCWxvY2FsaG9zdDBZMBMGByqGSM49AgEG
CCqGSM49AwEHA0IABDfMVtl2CR5acj7HWS3/IG7ufPkGkXTQrRS192giWWKSTuUA
2CMR/+ov0jRdXRa9iojCa3cNVc2KKg76Aci07f+jgaowgacwCQYDVR0TBAIwADAd
BgNVHQ4EFgQUUGGlj9QH2deCAQzlZX+MY0anE74wbgYDVR0jBGcwZYAUnW0gJEkB
PyvLeLUZvH4kydv7NnyhQqRAMD4xCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQb2xh
clNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBFQyBDQYIJAMFD4n5iQ8zoMAsG
```

A1UdDwQEAwIHgDAKBggqhkjOPQQDAgNpADBmAjEAzp4DkFMq7eDB0x5FeS9gYDaG
Ol8rVnWlRTLQzHZBQjKp+TcBdHZaBPoi8LyXtWA4AjEA6OWhsuTcv/qXOscQT0rL
eEh8wcCQeJK1uNd78lNvx3W0Pcxdb6cd7AhaAKgXL+r4
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDCjCCAfKgAwIBAgIBATANBgkqhkiG9w0BAQsFADAmMSQwIgYDVQQDExtUZXN0
IGludGVybWVkaWF0ZSBtYXhwYXRoIDEwHhcNMDEwMTAxMDAwMDAwWhcNMzAxMjMx
MjM1OTU5WjAcMRowGAYDVQQDExFUZXN0IExlYWYgdmFsaWQgMzCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAIoBoBxjVjZBFlhZ+3mlOJAtlo0d0bXAbKFt
TJUJ3VL8FlB4HG3yIO54eujoul5dyKgDIx49SdBDxnME35i3Wkbzd/Co0zId/xYh
a61C9DDYIhsY5E7YVoLH1eAv4t70Q0wlvtlDBXXevs+4cBX/pXU7Aj/UKfvdxna7
Ja7wEdltKoxy1CwCRpP+ls8RRusXgoHYZKKAz6a7H5WSf3DdUrqk2DmlTAI/SWqL
0rVE1YRfKLg1C6atH4gSJqJXTm3BnWgFpYEZdJPDXaEi6Vnf+/oYuLB+T0jmavvI
NZUN3IKxO7WuF96f4ungKXJ9YchJE8vWaSjhb2V5zOA9Y/PikikCAwEAAaNNMEsw
CQYDVR0TBAIwADAdBgNVHQ4EFgQUwjdrwy2NbXHp088kZpUuEwXtsYowHwYDVR0j
BBgwFoAUOBl8edVm/H5xdS2EGEeLzftZ/DUwDQYJKoZIhvcNAQELBQADggEBAK9R
J7H8epG2NagZ3Gpl6R1jSiIixWlPJci2Bz1Nr8NIER64TJCKHeh9ku6tzSdrVL3B
2rj5GmpubDXEWAKfMtt0ccF2UIva9rDMNzaAnCSevWHXf9Httr84X6RmhtXb9/Rm
fp3W+L0GlDfHfHn8uoVdQe5e6xkmGxtcHDUsyO/CJMkrwUyoB8zs7UtlNtOf45H4
PPg09lzV7RQ9vFIH48F/4gZW+w3AqN9ZwvYkGcJUY8tyHpb9hDrR4F6loVInrlCE
0pQiQXNCdee1za9QsScSjYNxGfR2Dkzote41H098jvLalLTTg5Fqx/AylnX285FI
ETGOumNQ51IJLUpq+hc=
-----END
CERTIFICATE-----
BLOWFISH Encrypt and decrypt 0 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:0:-1

BLOWFISH Encrypt and decrypt 1 byte
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:1:-1

BLOWFISH Encrypt and decrypt 2 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:2:-1

BLOWFISH Encrypt and decrypt 7 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:7:-1

BLOWFISH Encrypt and decrypt 8 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:8:-1

BLOWFISH Encrypt and decrypt 9 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:9:-1

BLOWFISH
Encrypt and decrypt 15 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:15:-1

BLOWFISH Encrypt and decrypt 16 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:16:-1

BLOWFISH Encrypt and decrypt 17 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:17:-1

BLOWFISH Encrypt and decrypt 31 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:31:-1

BLOWFISH Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:32:-1

BLOWFISH
Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:33:-1

BLOWFISH Encrypt and decrypt 47 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:47:-1

BLOWFISH Encrypt and decrypt 48 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:48:-1

BLOWFISH Encrypt and decrypt 49 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:49:-1

BLOWFISH Encrypt and decrypt 0 bytes with one and zeros padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:0:MBEDTLS_PADDING_ONE_AND_ZEROS

BLOWFISH
Encrypt and decrypt 1 byte with one and zeros padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:1:MBEDTLS_PADDING_ONE_AND_ZEROS

BLOWFISH Encrypt and decrypt 2 bytes with one and zeros padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:2:MBEDTLS_PADDING_ONE_AND_ZEROS

BLOWFISH Encrypt and decrypt 7 bytes with one and zeros padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:7:MBEDTLS_PADDING_ONE_AND_ZEROS

BLOWFISH Encrypt and decrypt 8 bytes with one and zeros padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:8:MBEDTLS_PADDING_ONE_AND_ZEROS

BLOWFISH Encrypt
and decrypt 9 bytes with one and zeros padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:9:MBEDTLS_PADDING_ONE_AND_ZEROS

BLOWFISH Encrypt and decrypt 15 bytes with one and zeros padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:15:MBEDTLS_PADDING_ONE_AND_ZEROS

BLOWFISH Encrypt and decrypt 16 bytes with one and zeros padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:16:MBEDTLS_PADDING_ONE_AND_ZEROS

BLOWFISH Encrypt and decrypt 17 bytes with one and zeros padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:17:MBEDTLS_PADDING_ONE_AND_ZEROS

BLOWFISH Encrypt and decrypt 31 bytes with one and zeros
padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:31:MBEDTLS_PADDING_ONE_AND_ZEROS

BLOWFISH Encrypt and decrypt 32 bytes with one and zeros padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:32:MBEDTLS_PADDING_ONE_AND_ZEROS

BLOWFISH Encrypt and decrypt 32 bytes with one and zeros padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:33:MBEDTLS_PADDING_ONE_AND_ZEROS

BLOWFISH Encrypt and decrypt 47 bytes with one and zeros padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:47:MBEDTLS_PADDING_ONE_AND_ZEROS

BLOWFISH Encrypt and decrypt 48 bytes with one and zeros padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:48:MBEDTLS_PADDING_ONE_AND_ZEROS

BLOWFISH
Encrypt and decrypt 49 bytes with one and zeros padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7

enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:49:MBEDTLS_PADDING_ONE_AND_ZEROS

BLOWFISH Encrypt and decrypt 0 bytes with zeros and len padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:0:MBEDTLS_PADDING_ZEROS_AND_LEN

BLOWFISH Encrypt and decrypt 1 byte with zeros and len padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:1:MBEDTLS_PADDING_ZEROS_AND_LEN

BLOWFISH Encrypt and decrypt 2 bytes with zeros and len padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:2:MBEDTLS_PADDING_ZEROS_AND_LEN

BLOWFISH
Encrypt and decrypt 7 bytes with zeros and len padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:7:MBEDTLS_PADDING_ZEROS_AND_LEN

BLOWFISH Encrypt and decrypt 8 bytes with zeros and len padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:8:MBEDTLS_PADDING_ZEROS_AND_LEN

BLOWFISH Encrypt and decrypt 9 bytes with zeros and len padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:9:MBEDTLS_PADDING_ZEROS_AND_LEN

BLOWFISH Encrypt and decrypt 15 bytes with zeros and len padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:15:MBEDTLS_PADDING_ZEROS_AND_LEN

BLOWFISH

Encrypt and decrypt 16 bytes with zeros and len padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:16:MBEDTLS_PADDING_ZEROS_AND_LEN

BLOWFISH Encrypt and decrypt 17 bytes with zeros and len padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:17:MBEDTLS_PADDING_ZEROS_AND_LEN

BLOWFISH Encrypt and decrypt 31 bytes with zeros and len padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:31:MBEDTLS_PADDING_ZEROS_AND_LEN

BLOWFISH Encrypt and decrypt 32 bytes with zeros and len padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:32:MBEDTLS_PADDING_ZEROS_AND_LEN

BLOWFISH
Encrypt and decrypt 32 bytes with zeros and len padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:33:MBEDTLS_PADDING_ZEROS_AND_LEN

BLOWFISH Encrypt and decrypt 47 bytes with zeros and len padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:47:MBEDTLS_PADDING_ZEROS_AND_LEN

BLOWFISH Encrypt and decrypt 48 bytes with zeros and len padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:48:MBEDTLS_PADDING_ZEROS_AND_LEN

BLOWFISH Encrypt and decrypt 49 bytes with zeros and len padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:49:MBEDTLS_PADDING_ZEROS_AND_LEN

BLOWFISH
Encrypt and decrypt 0 bytes with zeros padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:0:MBEDTLS_PADDING_ZEROS

BLOWFISH Encrypt and decrypt 1 byte with zeros padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:1:MBEDTLS_PADDING_ZEROS

BLOWFISH Encrypt and decrypt 2 bytes with zeros padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:2:MBEDTLS_PADDING_ZEROS

BLOWFISH Encrypt and decrypt 7 bytes with zeros padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:7:MBEDTLS_PADDING_ZEROS

BLOWFISH Encrypt and decrypt 8 bytes with zeros padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:8:MBEDTLS_PADDING_ZEROS

BLOWFISH
Encrypt and decrypt 9 bytes with zeros padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:9:MBEDTLS_PADDING_ZEROS

BLOWFISH Encrypt and decrypt 15 bytes with zeros padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:15:MBEDTLS_PADDING_ZEROS

BLOWFISH Encrypt and decrypt 16 bytes with zeros padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7

enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-
CBC":128:16:MBEDTLS_PADDING_ZEROS

BLOWFISH Encrypt and decrypt 17 bytes with zeros padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-
CBC":128:17:MBEDTLS_PADDING_ZEROS

BLOWFISH
Encrypt and decrypt 31 bytes with zeros padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-
CBC":128:31:MBEDTLS_PADDING_ZEROS

BLOWFISH Encrypt and decrypt 32 bytes with zeros padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-
CBC":128:32:MBEDTLS_PADDING_ZEROS

BLOWFISH Encrypt and decrypt 32 bytes with zeros padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-
CBC":128:33:MBEDTLS_PADDING_ZEROS

BLOWFISH Encrypt and decrypt 47 bytes with zeros padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-
CBC":128:47:MBEDTLS_PADDING_ZEROS

BLOWFISH Encrypt and decrypt 48 bytes with zeros padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-
CBC":128:48:MBEDTLS_PADDING_ZEROS

BLOWFISH
Encrypt and decrypt 49 bytes with zeros padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-
CBC":128:49:MBEDTLS_PADDING_ZEROS

BLOWFISH Encrypt and decrypt 0 bytes with no padding

depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:0:MBEDTLS_PADDING_NONE

BLOWFISH Encrypt and decrypt 8 bytes with no padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:8:MBEDTLS_PADDING_NONE

BLOWFISH Encrypt and decrypt 16 bytes with no padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:16:MBEDTLS_PADDING_NONE

BLOWFISH
Encrypt and decrypt 32 bytes with no padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:32:MBEDTLS_PADDING_NONE

BLOWFISH Encrypt and decrypt 48 bytes with no padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":128:48:MBEDTLS_PADDING_NONE

BLOWFISH Try encrypting 1 bytes with no padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_BLOWFISH_CBC:MBEDTLS_PADDING_NONE:128:1:MBEDTLS_ERR_CIPHER_FULL_BLOCK_EXPECTED

BLOWFISH Try encrypting 2 bytes with no padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_BLOWFISH_CBC:MBEDTLS_PADDING_NONE:128:2:MBEDTLS_ERR_CIPHER_FULL_BLOCK_EXPECTED

BLOWFISH Try encrypting 7 bytes with no padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_BLOWFISH_CBC:MBEDTLS_PADDING_NONE:128:7:MBEDTLS_ERR_CIPHER_FULL_BLOCK_EXPECTED

BLOWFISH

Try encrypting 9 bytes with no padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_BLOWFISH_CBC:MBEDTLS_PADDING_NONE:128:9:MBEDTLS_ERR_CIPHER_FULL_BLOCK_EXPECTED

BLOWFISH Try encrypting 15 bytes with no padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_BLOWFISH_CBC:MBEDTLS_PADDING_NONE:128:15:MBEDTLS_ERR_CIPHER_FULL_BLOCK_EXPECTED

BLOWFISH Try encrypting 17 bytes with no padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_BLOWFISH_CBC:MBEDTLS_PADDING_NONE:128:17:MBEDTLS_ERR_CIPHER_FULL_BLOCK_EXPECTED

BLOWFISH Try encrypting 31 bytes with no padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_BLOWFISH_CBC:MBEDTLS_PADDING_NONE:128:31:MBEDTLS_ERR_CIPHER_FULL_BLOCK_EXPECTED

BLOWFISH
Try encrypting 33 bytes with no padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_BLOWFISH_CBC:MBEDTLS_PADDING_NONE:128:33:MBEDTLS_ERR_CIPHER_FULL_BLOCK_EXPECTED

BLOWFISH Try encrypting 47 bytes with no padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_BLOWFISH_CBC:MBEDTLS_PADDING_NONE:128:47:MBEDTLS_ERR_CIPHER_FULL_BLOCK_EXPECTED

BLOWFISH Try encrypting 49 bytes with no padding
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_BLOWFISH_CBC:MBEDTLS_PADDING_NONE:128:49:MBEDTLS_ERR_CIPHER_FULL_BLOCK_EXPECTED

BLOWFISH Encrypt and decrypt 0 bytes in multiple parts
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CBC:128:0:0:

BLOWFISH
Encrypt and decrypt 1 bytes in multiple parts 1
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CBC:128:1:0:

BLOWFISH Encrypt and decrypt 1 bytes in multiple parts 2
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CBC:128:0:1:

BLOWFISH Encrypt and decrypt 16 bytes in multiple parts 1
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CBC:128:16:0:

BLOWFISH Encrypt and decrypt 16 bytes in multiple parts 2
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CBC:128:0:16:

BLOWFISH Encrypt and decrypt 16 bytes in multiple parts 3
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CBC:128:1:15:

BLOWFISH
Encrypt and decrypt 16 bytes in multiple parts 4
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CBC:128:15:1:

BLOWFISH Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CBC:128:15:7:

BLOWFISH Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CBC:128:16:6:

BLOWFISH Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CBC:128:17:6:

BLOWFISH Encrypt and decrypt 32 bytes in multiple parts 1

depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CBC:128:16:16:

BLOWFISH
Encrypt and decrypt 0 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CFB64:"BLOWFISH-CFB64":128:0:-1

BLOWFISH Encrypt and decrypt 1 byte
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CFB64:"BLOWFISH-CFB64":128:1:-1

BLOWFISH Encrypt and decrypt 2 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CFB64:"BLOWFISH-CFB64":128:2:-1

BLOWFISH Encrypt and decrypt 7 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CFB64:"BLOWFISH-CFB64":128:7:-1

BLOWFISH Encrypt and decrypt 8 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CFB64:"BLOWFISH-CFB64":128:8:-1

BLOWFISH Encrypt and decrypt 9 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CFB64:"BLOWFISH-CFB64":128:9:-1

BLOWFISH
Encrypt and decrypt 15 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CFB64:"BLOWFISH-CFB64":128:15:-1

BLOWFISH Encrypt and decrypt 16 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CFB64:"BLOWFISH-CFB64":128:16:-1

BLOWFISH Encrypt and decrypt 17 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CFB64:"BLOWFISH-CFB64":128:17:-1

BLOWFISH Encrypt and decrypt 31 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CFB64:"BLOWFISH-CFB64":128:31:-1

BLOWFISH Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CFB

enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CFB64:"BLOWFISH-CFB64":128:32:-1

BLOWFISH Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CFB64:"BLOWFISH-CFB64":128:33:-1

BLOWFISH Encrypt and decrypt 47 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CFB64:"BLOWFISH-CFB64":128:47:-1

BLOWFISH
Encrypt and decrypt 48 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CFB64:"BLOWFISH-CFB64":128:48:-1

BLOWFISH Encrypt and decrypt 49 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CFB64:"BLOWFISH-CFB64":128:49:-1

BLOWFISH Encrypt and decrypt 0 bytes in multiple parts
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CFB64:128:0:0:

BLOWFISH Encrypt and decrypt 1 bytes in multiple parts 1
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CFB64:128:1:0:

BLOWFISH Encrypt and decrypt 1 bytes in multiple parts 2
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CFB64:128:0:1:

BLOWFISH Encrypt and decrypt 16
bytes in multiple parts 1
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CFB64:128:16:0:

BLOWFISH Encrypt and decrypt 16 bytes in multiple parts 2
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CFB64:128:0:16:

BLOWFISH Encrypt and decrypt 16 bytes in multiple parts 3
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CFB64:128:1:15:

BLOWFISH Encrypt and decrypt 16 bytes in multiple parts 4
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CFB64:128:15:1:

BLOWFISH Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CFB64:128:15:7:

BLOWFISH Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CFB64:128:16:6:

BLOWFISH
Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CFB64:128:17:6:

BLOWFISH Encrypt and decrypt 32 bytes in multiple parts 1
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CFB64:128:16:16:

BLOWFISH Encrypt and decrypt 0 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CTR:"BLOWFISH-CTR":128:0:-1

BLOWFISH Encrypt and decrypt 1 byte
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CTR:"BLOWFISH-CTR":128:1:-1

BLOWFISH Encrypt and decrypt 2 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CTR:"BLOWFISH-CTR":128:2:-1

BLOWFISH Encrypt and decrypt 7 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CTR:"BLOWFISH-CTR":128:7:-1

BLOWFISH
Encrypt and decrypt 8 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CTR:"BLOWFISH-CTR":128:8:-1

BLOWFISH Encrypt and decrypt 9 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CTR:"BLOWFISH-CTR":128:9:-1

BLOWFISH Encrypt and decrypt 15 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CTR:"BLOWFISH-CTR":128:15:-1

BLOWFISH Encrypt and decrypt 16 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CTR

enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CTR:"BLOWFISH-CTR":128:16:-1

BLOWFISH Encrypt and decrypt 17 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CTR:"BLOWFISH-CTR":128:17:-1

BLOWFISH Encrypt and decrypt 31 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CTR:"BLOWFISH-CTR":128:31:-1

BLOWFISH Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CTR:"BLOWFISH-CTR":128:32:-1

BLOWFISH
Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CTR:"BLOWFISH-CTR":128:33:-1

BLOWFISH Encrypt and decrypt 47 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CTR:"BLOWFISH-CTR":128:47:-1

BLOWFISH Encrypt and decrypt 48 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CTR:"BLOWFISH-CTR":128:48:-1

BLOWFISH Encrypt and decrypt 49 bytes
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CTR:"BLOWFISH-CTR":128:49:-1

BLOWFISH Encrypt and decrypt 0 bytes in multiple parts
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CTR:128:0:0:

BLOWFISH Encrypt and decrypt 1 bytes in multiple parts 1
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CTR:128:1:0:

BLOWFISH
Encrypt and decrypt 1 bytes in multiple parts 2
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CTR:128:0:1:

BLOWFISH Encrypt and decrypt 16 bytes in multiple parts 1
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CTR:128:16:0:

BLOWFISH Encrypt and decrypt 16 bytes in multiple parts 2
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CTR:128:0:16:

BLOWFISH Encrypt and decrypt 16 bytes in multiple parts 3
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CTR:128:1:15:

BLOWFISH Encrypt and decrypt 16 bytes in multiple parts 4
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CTR:128:15:1:

BLOWFISH Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CTR:128:15:7:

BLOWFISH
Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CTR:128:16:6:

BLOWFISH Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CTR:128:17:6:

BLOWFISH Encrypt and decrypt 32 bytes in multiple parts 1
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_BLOWFISH_CTR:128:16:16:

BLOWFISH CBC Encrypt and decrypt 7 bytes, 192-bits key
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CBC:"BLOWFISH-CBC":192:7:-1

BLOWFISH CTR Encrypt and decrypt 7 bytes, 192-bits key
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CTR:"BLOWFISH-CTR":192:7:-1

BLOWFISH
CFB64 Encrypt and decrypt 7 bytes, 192-bits key
depends_on:MBEDTLS_BLOWFISH_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_BLOWFISH_CFB64:"BLOWFISH-CFB64":192:7:-1

BLOWFISH ECB Encrypt test vector (SSLeay) #1
depends_on:MBEDTLS_BLOWFISH_C
test_vec_ecb:MBEDTLS_CIPHER_BLOWFISH_ECB:MBEDTLS_ENCRYPT:"00000000000000000000000000000000":"0000000000000000":"4ef997456198dd78":0

BLOWFISH ECB Encrypt test vector (SSLeay) #2
depends_on:MBEDTLS_BLOWFISH_C
test_vec_ecb:MBEDTLS_CIPHER_BLOWFISH_ECB:MBEDTLS_ENCRYPT:"ffffffffffffffffffffffffffffffff":"ffffffffffffffff":"51866fd5b85ecb8a":0

BLOWFISH ECB Encrypt test vector (SSLeay) #3
depends_on:MBEDTLS_BLOWFISH_C
test_vec_ecb:MBEDTLS_CIPHER_BLOWFISH_ECB:MBEDTLS_ENCRYPT:"fedcba9876543210fedcba9876543210":"0123456789abcdef":"0aceab0fc6a0a28d":0

BLOWFISH ECB Encrypt test vector (SSLeay) #3, 64-bit key
depends_on:MBEDTLS_BLOWFISH_C
test_vec_ecb:MBEDTLS_CIPHER_BLOWFISH_ECB:MBEDTLS_ENCRYPT:"fedcba9876543210":"0123456789abcdef":"0aceab0fc6a0a28d":0

BLOWFISH
ECB Encrypt test vector (SSLeay) #3, 192-bit key
depends_on:MBEDTLS_BLOWFISH_C
test_vec_ecb:MBEDTLS_CIPHER_BLOWFISH_ECB:MBEDTLS_ENCRYPT:"fedcba9876543210fedcba9876543210fedcba9876543210":"0123456789abcdef":"0aceab0fc6a0a28d":0

BLOWFISH ECB Decrypt test vector (SSLeay) #1
depends_on:MBEDTLS_BLOWFISH_C
test_vec_ecb:MBEDTLS_CIPHER_BLOWFISH_ECB:MBEDTLS_DECRYPT:"00000000000000000000000000000000":"4ef997456198dd78":"0000000000000000":0

BLOWFISH ECB Decrypt test vector (SSLeay) #2
depends_on:MBEDTLS_BLOWFISH_C
test_vec_ecb:MBEDTLS_CIPHER_BLOWFISH_ECB:MBEDTLS_DECRYPT:"ffffffffffffffffffffffffffffffff":"51866fd5b85ecb8a":"ffffffffffffffff":0

BLOWFISH ECB Decrypt test vector (SSLeay) #3
depends_on:MBEDTLS_BLOWFISH_C
test_vec_ecb:MBEDTLS_CIPHER_BLOWFISH_ECB:MBEDTLS_DECRYPT:"3849674c2602319e3849674c2602319e":"a25e7856cf2651eb":"51454b582ddf440a":0

BLOWFISH ECB Decrypt test vector (SSLeay) #3, 64-bit key
depends_on:MBEDTLS_BLOWFISH_C
test_vec_ecb:MBEDTLS_CIPHER_BLOWFISH_ECB:MBEDTLS_DECRYPT:"3849674c2602319e":"a25e7856cf2651eb":"51454b582ddf440a":0

BLOWFISH
ECB Decrypt test vector (SSLeay) #3, 192-bit key
depends_on:MBEDTLS_BLOWFISH_C
test_vec_ecb:MBEDTLS_CIPHER_BLOWFISH_ECB:MBEDTLS_DECRYPT:"3849674c2602319e3849674c2602319e3849674c2602319e":"a25e7856cf2651eb":"51454b582ddf440a":0
AES-128-CCM test vector NIST #1 (P=0, N=7, A=0, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C

auth_crypt_tv:MBEDTLS_CIPHER_AES_128_CCM:"4ae701103c63deca5b5a3939d7d05992":"5a8aa485c316e9":
"":"":"02209f55":""

AES-128-CCM test vector NIST #2 (P=0, N=7, A=0, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_128_CCM:"4ae701103c63deca5b5a3939d7d05992":"3796cf51b87266":
"":"":"9a04c241":"FAIL"

AES-128-CCM test vector NIST #3 (P=0, N=7, A=0, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_128_CCM:"4bb3c4a4f893ad8c9bdc833c325d62b3":"5a8aa485c316e9":"
":"":"75d582db43ce9b13ab4b6f7f14341330":""

AES-128-CCM test vector NIST #4 (P=0, N=7, A=0, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_128_CCM:"4bb3c4a4f893ad8c9bdc833c325d62b3":"3796cf51b87266":
"":"":"3a65e03af37b81d05acc7ec1bc39deb0":"FAIL"

AES-128-CCM test vector NIST #5 (P=0, N=13, A=0, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_128_CCM:"4bb3c4a4f893ad8c9bdc833c325d62b3":"5a8aa485c316e940
3aff859fbb":"":"":"90156f3f":""

AES-128-CCM
test vector NIST #6 (P=0, N=13, A=0, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_128_CCM:"4bb3c4a4f893ad8c9bdc833c325d62b3":"a16a2e741f1cd971
7285b6d882":"":"":"88909016":"FAIL"

AES-128-CCM test vector NIST #7 (P=0, N=13, A=0, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_128_CCM:"19ebfde2d5468ba0a3031bde629b11fd":"5a8aa485c316e940
3aff859fbb":"":"":"fb04dc5a44c6bb000f2440f5154364b4":""

AES-128-CCM test vector NIST #8 (P=0, N=13, A=0, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_128_CCM:"19ebfde2d5468ba0a3031bde629b11fd":"a16a2e741f1cd971
7285b6d882":"":"":"5447075bf42a59b91f08064738b015ab":"FAIL"

AES-128-CCM test vector NIST #9 (P=24, N=7, A=0, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_128_CCM:"19ebfde2d5468ba0a3031bde629b11fd":"5a8aa485c316e9":"
":"a90e8ea44085ced791b2fdb7fd44b5cf0bd7d27718029bb7":"03e1fa6b":"3796cf51b8726652a4204733b8fbb047cf
00fb91a9837e22"

AES-128-CCM
test vector NIST #10 (P=24, N=7, A=0, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C

auth_crypt_tv:MBEDTLS_CIPHER_AES_128_CCM:"19ebfde2d5468ba0a3031bde629b11fd":"31f8fa25827d48":"":"50aafe0578c115c4a8e126ff7b3ccb64dce8ccaa8ceda69f":"23e5d81c":"FAIL"

AES-128-CCM test vector NIST #11 (P=24, N=7, A=0, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_128_CCM:"197afb02ffbd8f699dacae87094d5243":"5a8aa485c316e9":"":"24ab9eeb0e5508cae80074f1070ee188a637171860881f1f":"2d9a3fbc210595b7b8b1b41523111a8e":"3796cf51b8726652a4204733b8fbb047cf00fb91a9837e22"

AES-128-CCM test vector NIST #12 (P=24, N=7, A=0, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_128_CCM:"197afb02ffbd8f699dacae87094d5243":"31f8fa25827d48":"":"7ebfda6fa5da1dbffd82dc29b875798fbcef8ba0084fbd24":"63af747cc88a001fa94e060290f209c4":"FAIL"

AES-128-CCM
test vector NIST #13 (P=24, N=13, A=0, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_128_CCM:"197afb02ffbd8f699dacae87094d5243":"5a8aa485c316e9403aff859fbb":"":"4a550134f94455979ec4bf89ad2bd80d25a77ae94e456134":"a3e138b9":"a16a2e741f1cd9717285b6d882c1fc53655e9773761ad697"

AES-128-CCM test vector NIST #14 (P=24, N=13, A=0, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_128_CCM:"197afb02ffbd8f699dacae87094d5243":"49004912fdd7269279b1f06a89":"":"118ec53dd1bfbe52d5b9fe5dfebecf2ee674ec983eada654":"091a5ae9":"FAIL"

AES-128-CCM test vector NIST #15 (P=24, N=13, A=0, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_128_CCM:"90929a4b0ac65b350ad1591611fe4829":"5a8aa485c316e9403aff859fbb":"":"4bfe4e35784f0a65b545477e5e2f4bae0e1e6fa717eaf2cb":"6a9a970b9beb2ac1bd4fd62168f8378a":"a16a2e741f1cd9717285b6d882c1fc53655e9773761ad697"

AES-128-CCM test vector NIST #16 (P=24, N=13, A=0, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_128_CCM:"90929a4b0ac65b350ad1591611fe4829":"49004912fdd7269279b1f06a89":"":"0c56a503aa2c12e87450d45a7b714db980fd348f327c0065":"a65666144994bad0c8195bcb4ade1337":"FAIL"

AES-128-CCM
test vector NIST #17 (P=0, N=7, A=32, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_128_CCM:"90929a4b0ac65b350ad1591611fe4829":"5a8aa485c316e9":"3796cf51b8726652a4204733b8fbb047cf00fb91a9837e22ec22b1a268f88e2c":"":"782e4318":""

AES-128-CCM test vector NIST #18 (P=0, N=7, A=32, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_128_CCM:"90929a4b0ac65b350ad1591611fe4829":"a265480ca88d5f":"a2248a882ecbf850daf91933a389e78e81623d233dfd47bf8321361a38f138fe":"":"a04f270a":"FAIL"

AES-128-CCM test vector NIST #19 (P=0, N=7, A=32, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_128_CCM:"6a798d7c5e1a72b43e20ad5c7b08567b":"5a8aa485c316e9":"3796cf51b8726652a4204733b8fbb047cf00fb91a9837e22ec22b1a268f88e2c":"":"41b476013f45e4a781f253a6f3b1e530":""

AES-128-CCM
test vector NIST #20 (P=0, N=7, A=32, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_128_CCM:"6a798d7c5e1a72b43e20ad5c7b08567b":"a265480ca88d5f":"a2248a882ecbf850daf91933a389e78e81623d233dfd47bf8321361a38f138fe":"":"f9f018fcd125822616083fffebc4c8e6":"FAIL"

AES-128-CCM test vector NIST #21 (P=0, N=13, A=32, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_128_CCM:"6a798d7c5e1a72b43e20ad5c7b08567b":"5a8aa485c316e9403aff859fbb":"a16a2e741f1cd9717285b6d882c1fc53655e9773761ad697a7ee6410184c7982":"":"9f69f24f":""

AES-128-CCM test vector NIST #22 (P=0, N=13, A=32, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_128_CCM:"6a798d7c5e1a72b43e20ad5c7b08567b":"8739b4bea1a099fe547499cbc6":"f6107696edb332b2ea059d8860fee26be42e5e12e1a4f79a8d0eafce1b2278a7":"":"e17afaa4":"FAIL"

AES-128-CCM test vector NIST #23 (P=0, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_128_CCM:"f9fdca4ac64fe7f014de0f43039c7571":"5a8aa485c316e9403aff859fbb":"a16a2e741f1cd9717285b6d882c1fc53655e9773761ad697a7ee6410184c7982":"":"1859ac36a40a6b28b34266253627797a":""

AES-128-CCM
test vector NIST #24 (P=0, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_128_CCM:"f9fdca4ac64fe7f014de0f43039c7571":"8739b4bea1a099fe547499cbc6":"f6107696edb332b2ea059d8860fee26be42e5e12e1a4f79a8d0eafce1b2278a7":"":"edf8b46eb69ac0044116019dec183072":"FAIL"

AES-128-CCM test vector NIST #25 (P=24, N=7, A=32, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_128_CCM:"f9fdca4ac64fe7f014de0f43039c7571":"5a8aa485c316e9":"3796cf51b8726652a4204733b8fbb047cf00fb91a9837e22ec22b1a268f88e2c":"6be31860ca271ef448de8f8d8b39346daf4b81d7e92d65b3":"38f125fa":"a265480ca88d5f536db0dc6abc40faf0d05be7a966977768"

AES-128-CCM test vector NIST #26 (P=24, N=7, A=32, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_128_CCM:"f9fdca4ac64fe7f014de0f43039c7571":"fdd2d6f503c915":"5b92394f21ddc3ad49d9b0881b829a5935cb3a4d23e292a62fb66b5e7ab7020e":"4cc57a9927a6bc401441870d3193bf89ebd163f5c01501c7":"28a66b69":"FAIL"

AES-128-CCM
test vector NIST #27 (P=24, N=7, A=32, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_128_CCM:"a7aa635ea51b0bb20a092bd5573e728c":"5a8aa485c316e9":"3796cf51b8726652a4204733b8fbb047cf00fb91a9837e22ec22b1a268f88e2c":"b351ab96b2e45515254558d5212673ee6c776d42dbca3b51":"2cf3a20b7fd7c49e6e79bef475c2906f":"a265480ca88d5f536db0dc6abc40faf0d05be7a966977768"

AES-128-CCM test vector NIST #28 (P=24, N=7, A=32, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_128_CCM:"a7aa635ea51b0bb20a092bd5573e728c":"fdd2d6f503c915":"5b92394f21ddc3ad49d9b0881b829a5935cb3a4d23e292a62fb66b5e7ab7020e":"df1a5285caa41b4bb47f6e5ceceba4e82721828d68427a30":"81d18ca149d6766bfaccec88f194eb5b":"FAIL"

AES-128-CCM
test vector NIST #29 (P=24, N=13, A=32, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_128_CCM:"a7aa635ea51b0bb20a092bd5573e728c":"5a8aa485c316e9403aff859fbb":"a16a2e741f1cd9717285b6d882c1fc53655e9773761ad697a7ee6410184c7982":"934f893824e880f743d196b22d1f340a52608155087bd28a":"c25e5329":"8739b4bea1a099fe547499cbc6d1b13d849b8084c9b6acc5"

AES-128-CCM test vector NIST #30 (P=24, N=13, A=32, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_128_CCM:"a7aa635ea51b0bb20a092bd5573e728c":"0812757ad0cc4d17c4cfe7a642":"ec6c44a7e94e51a3ca6dee229098391575ec7213c85267fbf7492fdbeee61b10":"f43ba9d834ad85dfab3f1c0c27c3441fe4e411a38a261a65":"59b3b3ee":"FAIL"

AES-128-CCM test vector NIST #31 (P=24, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_128_CCM:"26511fb51fcfa75cb4b44da75a6e5a0e":"5a8aa485c316e9403aff859fbb":"a16a2e741f1cd9717285b6d882c1fc53655e9773761ad697a7ee6410184c7982":"50038b5fdd364ee747b70d00bd36840ece4ea19998123375":"c0a458bfcafa3b2609afe0f825cbf503":"8739b4bea1a099fe547499cbc6d1b13d849b8084c9b6acc5"

AES-128-CCM
test vector NIST #32 (P=24, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_128_CCM:"26511fb51fcfa75cb4b44da75a6e5a0e":"0812757ad0cc4d17c4cfe7a642":"ec6c44a7e94e51a3ca6dee229098391575ec7213c85267fbf7492fdbeee61b10":"78ed8ff6b5a1255d0fbd0a719a9c27b059ff5f83d0c4962c":"390042ba8bb5f6798dab01c5afad7306":"FAIL"

AES-192-CCM test vector NIST #1 (P=0, N=7, A=0, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_192_CCM:"c98ad7f38b2c7e970c9b965ec87a08208384718f78206c6c":"5a8aa485c316e9":"":"":"9d4b7f3b":""

AES-192-CCM test vector NIST #2 (P=0, N=7, A=0, T=4)

depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_192_CCM:"c98ad7f38b2c7e970c9b965ec87a08208384718f78206c6c":"
3796cf51b87266":"":"":"80745de9":"FAIL"

AES-192-CCM test vector NIST #3 (P=0, N=7, A=0, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_192_CCM:"4bb3c4a4f893ad8c9bdc833c325d62b3d3ad1bccf9282a65":"
5a8aa485c316e9":"":"":"17223038fa99d53681ca1beabe78d1b4":""

AES-192-CCM
test vector NIST #4 (P=0, N=7, A=0, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_192_CCM:"4bb3c4a4f893ad8c9bdc833c325d62b3d3ad1bccf9282a65":"
3796cf51b87266":"":"":"d0e1eeef4d2a264536bb1c2c1bde7c35":"FAIL"

AES-192-CCM test vector NIST #5 (P=0, N=13, A=0, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_192_CCM:"4bb3c4a4f893ad8c9bdc833c325d62b3d3ad1bccf9282a65":"
5a8aa485c316e9403aff859fbb":"":"":"fe69ed84":""

AES-192-CCM test vector NIST #6 (P=0, N=13, A=0, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_192_CCM:"4bb3c4a4f893ad8c9bdc833c325d62b3d3ad1bccf9282a65":"
a16a2e741f1cd9717285b6d882":"":"":"db7ffc82":"FAIL"

AES-192-CCM test vector NIST #7 (P=0, N=13, A=0, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_192_CCM:"19ebfde2d5468ba0a3031bde629b11fd4094afcb205393fa":"
5a8aa485c316e9403aff859fbb":"":"":"0c66a8e547ed4f8c2c9a9a1eb5d455b9":""

AES-192-CCM
test vector NIST #8 (P=0, N=13, A=0, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_192_CCM:"19ebfde2d5468ba0a3031bde629b11fd4094afcb205393fa":"a
16a2e741f1cd9717285b6d882":"":"":"38757b3a61a4dc97ca3ab88bf1240695":"FAIL"

AES-192-CCM test vector NIST #9 (P=24, N=7, A=0, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_192_CCM:"19ebfde2d5468ba0a3031bde629b11fd4094afcb205393fa":"
5a8aa485c316e9":"":"411986d04d6463100bff03f7d0bde7ea2c3488784378138c":"ddc93a54":"3796cf51b8726652a
4204733b8fbb047cf00fb91a9837e22"

AES-192-CCM test vector NIST #10 (P=24, N=7, A=0, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_192_CCM:"19ebfde2d5468ba0a3031bde629b11fd4094afcb205393fa":"
31f8fa25827d48":"":"32b649ab56162e55d4148a1292d6a225a988eb1308298273":"b6889036":"FAIL"

AES-192-CCM

test vector NIST #11 (P=24, N=7, A=0, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_192_CCM:"197afb02ffbd8f699dacae87094d524324576b99844f75e1":"5a8aa485c316e9":"":"cba4b4aeb85f0492fd8d905c4a6d8233139833373ef188a8":"c5a5ebecf7ac8607fe412189e83d9d20":"3796cf51b8726652a4204733b8fbb047cf00fb91a9837e22"

AES-192-CCM test vector NIST #12 (P=24, N=7, A=0, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_192_CCM:"197afb02ffbd8f699dacae87094d524324576b99844f75e1":"31f8fa25827d48":"":"ca62713728b5c9d652504b0ae8fd4fee5d297ee6a8d19cb6":"e699f15f14d34dcaf9ba8ed4b877c97d":"FAIL"

AES-192-CCM test vector NIST #13 (P=24, N=13, A=0, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_192_CCM:"197afb02ffbd8f699dacae87094d524324576b99844f75e1":"5a8aa485c316e9403aff859fbb":"":"042653c674ef2a90f7fb11d30848e530ae59478f1051633a":"34fad277":"a16a2e741f1cd9717285b6d882c1fc53655e9773761ad697"

AES-192-CCM
test vector NIST #14 (P=24, N=13, A=0, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_192_CCM:"197afb02ffbd8f699dacae87094d524324576b99844f75e1":"49004912fdd7269279b1f06a89":"":"1902d9769a7ba3d3268e1257395c8c2e5f98eef295dcbfa5":"a35df775":"FAIL"

AES-192-CCM test vector NIST #15 (P=24, N=13, A=0, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_192_CCM:"90929a4b0ac65b350ad1591611fe48297e03956f6083e451":"5a8aa485c316e9403aff859fbb":"":"a5b7d8cca2069908d1ed88e6a9fe2c9bede3131dad54671e":"a7ade30a07d185692ab0ebdf4c78cf7a":"a16a2e741f1cd9717285b6d882c1fc53655e9773761ad697"

AES-192-CCM test vector NIST #16 (P=24, N=13, A=0, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_192_CCM:"90929a4b0ac65b350ad1591611fe48297e03956f6083e451":"49004912fdd7269279b1f06a89":"":"9a98617fb97a0dfe466be692272dcdaec1c5443a3b51312e":"f042c86363cc05afb98c66e16be8a445":"FAIL"

AES-192-CCM test vector NIST
#17 (P=0, N=7, A=32, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_192_CCM:"90929a4b0ac65b350ad1591611fe48297e03956f6083e451":"5a8aa485c316e9":"3796cf51b8726652a4204733b8fbb047cf00fb91a9837e22ec22b1a268f88e2c":"":"1d089a5f":""

AES-192-CCM test vector NIST #18 (P=0, N=7, A=32, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_192_CCM:"90929a4b0ac65b350ad1591611fe48297e03956f6083e451":"a265480ca88d5f":"a2248a882ecbf850daf91933a389e78e81623d233dfd47bf8321361a38f138fe":"":"2f46022a":"FAIL"

AES-192-CCM test vector NIST #19 (P=0, N=7, A=32, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_192_CCM:"6a798d7c5e1a72b43e20ad5c7b08567b12ab744b61c070e2":"5a8aa485c316e9":"3796cf51b8726652a4204733b8fbb047cf00fb91a9837e22ec22b1a268f88e2c":"":"5280a2137fee3deefcfe9b63a1199fb3":""

AES-192-CCM test vector NIST #20 (P=0, N=7, A=32, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_192_CCM:"6a798d7c5e1a72b43e20ad5c7b08567b12ab744b61c070e2":"a265480ca88d5f":"a2248a882ecbf850daf91933a389e78e81623d233dfd47bf8321361a38f138fe":"":"d40a7318c5f2d82f838c0beeefe0d598":"FAIL"

AES-192-CCM
test vector NIST #21 (P=0, N=13, A=32, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_192_CCM:"6a798d7c5e1a72b43e20ad5c7b08567b12ab744b61c070e2":"5a8aa485c316e9403aff859fbb":"a16a2e741f1cd9717285b6d882c1fc53655e9773761ad697a7ee6410184c7982":"":"5e0eaebd":""

AES-192-CCM test vector NIST #22 (P=0, N=13, A=32, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_192_CCM:"6a798d7c5e1a72b43e20ad5c7b08567b12ab744b61c070e2":"8739b4bea1a099fe547499cbc6":"f6107696edb332b2ea059d8860fee26be42e5e12e1a4f79a8d0eafce1b2278a7":"":"71b7fc33":"FAIL"

AES-192-CCM test vector NIST #23 (P=0, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_192_CCM:"f9fdca4ac64fe7f014de0f43039c757194d544ce5d15eed4":"5a8aa485c316e9403aff859fbb":"a16a2e741f1cd9717285b6d882c1fc53655e9773761ad697a7ee6410184c7982":"":"d07ccf9fdc3d33aa94cda3d230da707c":""

AES-192-CCM
test vector NIST #24 (P=0, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_192_CCM:"f9fdca4ac64fe7f014de0f43039c757194d544ce5d15eed4":"8739b4bea1a099fe547499cbc6":"f6107696edb332b2ea059d8860fee26be42e5e12e1a4f79a8d0eafce1b2278a7":"":"65fe32b649dc328c9f531584897e85b3":"FAIL"

AES-192-CCM test vector NIST #25 (P=24, N=7, A=32, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_192_CCM:"f9fdca4ac64fe7f014de0f43039c757194d544ce5d15eed4":"5a8aa485c316e9":"3796cf51b8726652a4204733b8fbb047cf00fb91a9837e22ec22b1a268f88e2c":"9f6ca4af9b159148c889a6584d1183ea26e2614874b05045":"75dea8d1":"a265480ca88d5f536db0dc6abc40faf0d05be7a966977768"

AES-192-CCM test vector NIST #26 (P=24, N=7, A=32, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_192_CCM:"f9fdca4ac64fe7f014de0f43039c757194d544ce5d15eed4":"fdd2d6f503c915":"5b92394f21ddc3ad49d9b0881b829a5935cb3a4d23e292a62fb66b5e7ab7020e":"84d8212e9cfc212

1252baa3b065b1edcf50497b9594db1eb":"d7965825":"FAIL"

AES-192-CCM
test vector NIST #27 (P=24, N=7, A=32, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_192_CCM:"a7aa635ea51b0bb20a092bd5573e728ccd4b3e8cdd2ab33d":"5a8aa485c316e9":"3796cf51b8726652a4204733b8fbb047cf00fb91a9837e22ec22b1a268f88e2c":"6aab64c4787599d8f213446beadb16e08dba60e97f56dbd1":"4d1d980d6fe0fb44b421992662b97975":"a265480ca88d5f536db0dc6abc40faf0d05be7a966977768"

AES-192-CCM test vector NIST #28 (P=24, N=7, A=32, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_192_CCM:"a7aa635ea51b0bb20a092bd5573e728ccd4b3e8cdd2ab33d":"fdd2d6f503c915":"5b92394f21ddc3ad49d9b0881b829a5935cb3a4d23e292a62fb66b5e7ab7020e":"4980b2ee49b1aaf393175f5ab9bae95ec7904557dfa20660":"3c51d36c826f01384100886198a7f6a3":"FAIL"

AES-192-CCM test vector NIST #29 (P=24, N=13, A=32, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_192_CCM:"a7aa635ea51b0bb20a092bd5573e728ccd4b3e8cdd2ab33d":"5a8aa485c316e9403aff859fbb":"a16a2e741f1cd9717285b6d882c1fc53655e9773761ad697a7ee6410184c7982":"16e543d0e20615ff0df15acd9927ddfe40668a54bb854ccc":"c25e9fce":"8739b4bea1a099fe547499cbc6d1b13d849b8084c9b6acc5"

AES-192-CCM
test vector NIST #30 (P=24, N=13, A=32, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_192_CCM:"a7aa635ea51b0bb20a092bd5573e728ccd4b3e8cdd2ab33d":"0812757ad0cc4d17c4cfe7a642":"ec6c44a7e94e51a3ca6dee229098391575ec7213c85267fbf7492fdbeee61b10":"df35b109caf690656ae278bbd8f8bba687a2ce11b105dae9":"8ecedb3e":"FAIL"

AES-192-CCM test vector NIST #31 (P=24, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_192_CCM:"26511fb51fcfa75cb4b44da75a6e5a0eb8d9c8f3b906f886":"5a8aa485c316e9403aff859fbb":"a16a2e741f1cd9717285b6d882c1fc53655e9773761ad697a7ee6410184c7982":"c5b0b2ef17498c5570eb335df4588032958ba3d69bf6f317":"8464a6f7fa2b76744e8e8d95691cecb8":"8739b4bea1a099fe547499cbc6d1b13d849b8084c9b6acc5"

AES-192-CCM
test vector NIST #32 (P=24, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_192_CCM:"26511fb51fcfa75cb4b44da75a6e5a0eb8d9c8f3b906f886":"0812757ad0cc4d17c4cfe7a642":"ec6c44a7e94e51a3ca6dee229098391575ec7213c85267fbf7492fdbeee61b10":"d1f0518929f4ae2f0543de2a7dfe4bb0110bb3057e524a1c":"06bd6dc2e6bcc3436cffb969ae900388":"FAIL"

AES-256-CCM test vector NIST #1 (P=0, N=7, A=0, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_256_CCM:"eda32f751456e33195f1f499cf2dc7c97ea127b6d488f211ccc5126fbb24afa6":"a544218dadd3c1":"":"":"469c90bb":""

AES-256-CCM test vector NIST #2 (P=0, N=7, A=0, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_256_CCM:"eda32f751456e33195f1f499cf2dc7c97ea127b6d488f211ccc5126fbb24afa6":"d3d5424e20fbec":"":"":"46a908ed":"FAIL"

AES-256-CCM test vector
NIST #3 (P=0, N=7, A=0, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_256_CCM:"e1b8a927a95efe94656677b692662000278b441c79e879dd5c0ddc758bdc9ee8":"a544218dadd3c1":"":"":"8207eb14d33855a52acceed17dbcbf6e":""

AES-256-CCM test vector NIST #4 (P=0, N=7, A=0, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_256_CCM:"e1b8a927a95efe94656677b692662000278b441c79e879dd5c0ddc758bdc9ee8":"d3d5424e20fbec":"":"":"60f8e127cb4d30db6df0622158cd931d":"FAIL"

AES-256-CCM test vector NIST #5 (P=0, N=13, A=0, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_256_CCM:"e1b8a927a95efe94656677b692662000278b441c79e879dd5c0ddc758bdc9ee8":"a544218dadd3c10583db49cf39":"":"":"8a19a133":""

AES-256-CCM test vector NIST #6 (P=0, N=13, A=0, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_256_CCM:"e1b8a927a95efe94656677b692662000278b441c79e879dd5c0ddc758bdc9ee8":"3c0e2815d37d844f7ac240ba9d":"":"":"2e317f1b":"FAIL"

AES-256-CCM
test vector NIST #7 (P=0, N=13, A=0, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_256_CCM:"af063639e66c284083c5cf72b70d8bc277f5978e80d9322d99f2fdc718cda569":"a544218dadd3c10583db49cf39":"":"":"97e1a8dd4259ccd2e431e057b0397fcf":""

AES-256-CCM test vector NIST #8 (P=0, N=13, A=0, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_256_CCM:"af063639e66c284083c5cf72b70d8bc277f5978e80d9322d99f2fdc718cda569":"3c0e2815d37d844f7ac240ba9d":"":"":"5a9596c511ea6a8671adefc4f2157d8b":"FAIL"

AES-256-CCM test vector NIST #9 (P=24, N=7, A=0, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_256_CCM:"af063639e66c284083c5cf72b70d8bc277f5978e80d9322d99f2fdc718cda569":"a544218dadd3c1":"":"64a1341679972dc5869fcf69b19d5c5ea50aa0b5e985f5b7":"22aa8d59":"d3d5424e20fbec43ae495353ed830271515ab104f8860c98"

AES-256-CCM test vector NIST #10 (P=24, N=7, A=0, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_256_CCM:"af063639e66c284083c5cf72b70d8bc277f5978e80d9322d99f2fdc718cda569":"bfcda8b5a2d0d2":"":"c5b7f802bffc498c1626e3774f1d9f94045dfd8e1a10a202":"77d00a75":"FAI

L"

AES-256-CCM
test vector NIST #11 (P=24, N=7, A=0, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_256_CCM:"f7079dfa3b5c7b056347d7e437bcded683abd6e2c9e069d333284082cbb5d453":"a544218dadd3c1":"":"bc51c3925a960e7732533e4ef3a4f69ee6826de952bcb0fd":"374f3bb6db8377ebfc79674858c4f305":"d3d5424e20fbec43ae495353ed830271515ab104f8860c98"

AES-256-CCM test vector NIST #12 (P=24, N=7, A=0, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_256_CCM:"f7079dfa3b5c7b056347d7e437bcded683abd6e2c9e069d333284082cbb5d453":"bfcda8b5a2d0d2":"":"afa1fa8e8a70e26b02161150556d604101fdf423f332c336":"3275f2a4907d51b734fe7238cebbd48f":"FAIL"

AES-256-CCM test vector NIST #13 (P=24, N=13, A=0, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_256_CCM:"f7079dfa3b5c7b056347d7e437bcded683abd6e2c9e069d333284082cbb5d453":"a544218dadd3c10583db49cf39":"":"63e00d30e4b08fd2a1cc8d70fab327b2368e77a93be4f412":"3d14fb3f":"3c0e2815d37d844f7ac240ba9d6e3a0b2a86f706e885959e"

AES-256-CCM
test vector NIST #14 (P=24, N=13, A=0, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_256_CCM:"f7079dfa3b5c7b056347d7e437bcded683abd6e2c9e069d333284082cbb5d453":"894dcaa61008eb8fb052c60d41":"":"bb5425b3869b76856ec58e39886fb6f6f2ac13fe44cb132d":"8d0c0099":"FAIL"

AES-256-CCM test vector NIST #15 (P=24, N=13, A=0, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_256_CCM:"1b0e8df63c57f05d9ac457575ea764524b8610ae5164e6215f426f5a7ae6ede4":"a544218dadd3c10583db49cf39":"":"f0050ad16392021a3f40207bed3521fb1e9f808f49830c42":"3a578d179902f912f9ea1afbce1120b3":"3c0e2815d37d844f7ac240ba9d6e3a0b2a86f706e885959e"

AES-256-CCM test vector NIST #16 (P=24, N=13, A=0, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_256_CCM:"1b0e8df63c57f05d9ac457575ea764524b8610ae5164e6215f426f5a7ae6ede4":"894dcaa61008eb8fb052c60d41":"":"c408190d0fbf5034f83b24a8ed9657331a7ce141de4fae76":"9084607b83bd06e6442eac8dacf583cc":"FAIL"

AES-256-CCM
test vector NIST #17 (P=0, N=7, A=32, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_256_CCM:"1b0e8df63c57f05d9ac457575ea764524b8610ae5164e6215f426f5a7ae6ede4":"a544218dadd3c1":"d3d5424e20fbec43ae495353ed830271515ab104f8860c988d15b6d36c038eab":"":"92d00fbe":""

AES-256-CCM test vector NIST #18 (P=0, N=7, A=32, T=4)

depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_256_CCM:"1b0e8df63c57f05d9ac457575ea764524b8610ae5164e6215f426f5a7ae6ede4":"78c46e3249ca28":"232e957c65ffa11988e830d4617d500f1c4a35c1221f396c41ab214f074ca2dc":"":"9143e5c4":"FAIL"

AES-256-CCM test vector NIST #19 (P=0, N=7, A=32, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_256_CCM:"a4bc10b1a62c96d459fbaf3a5aa3face7313bb9e1253e696f96a7a8e36801088":"a544218dadd3c1":"d3d5424e20fbec43ae495353ed830271515ab104f8860c988d15b6d36c038eab":"":"93af11a08379eb37a16aa2837f09d69d":""

AES-256-CCM
test vector NIST #20 (P=0, N=7, A=32, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_256_CCM:"a4bc10b1a62c96d459fbaf3a5aa3face7313bb9e1253e696f96a7a8e36801088":"78c46e3249ca28":"232e957c65ffa11988e830d4617d500f1c4a35c1221f396c41ab214f074ca2dc":"":"d19b0c14ec686a7961ca7c386d125a65":"FAIL"

AES-256-CCM test vector NIST #21 (P=0, N=13, A=32, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_256_CCM:"a4bc10b1a62c96d459fbaf3a5aa3face7313bb9e1253e696f96a7a8e36801088":"a544218dadd3c10583db49cf39":"3c0e2815d37d844f7ac240ba9d6e3a0b2a86f706e885959e09a1005e024f6907":"":"866d4227":""

AES-256-CCM test vector NIST #22 (P=0, N=13, A=32, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_256_CCM:"a4bc10b1a62c96d459fbaf3a5aa3face7313bb9e1253e696f96a7a8e36801088":"e8de970f6ee8e80ede933581b5":"89f8b068d34f56bc49d839d8e47b347e6dae737b903b278632447e6c0485d26a":"":"94cb1127":"FAIL"

AES-256-CCM
test vector NIST #23 (P=0, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_256_CCM:"8c5cf3457ff22228c39c051c4e05ed4093657eb303f859a9d4b0f8be0127d88a":"a544218dadd3c10583db49cf39":"3c0e2815d37d844f7ac240ba9d6e3a0b2a86f706e885959e09a1005e024f6907":"":"867b0d87cf6e0f718200a97b4f6d5ad5":""

AES-256-CCM test vector NIST #24 (P=0, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_256_CCM:"8c5cf3457ff22228c39c051c4e05ed4093657eb303f859a9d4b0f8be0127d88a":"e8de970f6ee8e80ede933581b5":"89f8b068d34f56bc49d839d8e47b347e6dae737b903b278632447e6c0485d26a":"":"677a040d46ee3f2b7838273bdad14f16":"FAIL"

AES-256-CCM test vector NIST #25 (P=24, N=7, A=32, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_256_CCM:"8c5cf3457ff22228c39c051c4e05ed4093657eb303f859a9d4b0f8be0127d88a":"a544218dadd3c1":"d3d5424e20fbec43ae495353ed830271515ab104f8860c988d15b6d36c038eab":"c2fe12658139f5d0dd22cadf2e901695b579302a72fc5608":"3ebc7720":"78c46e3249ca28e1ef0531d80fd37c124d9

aecb7be6668e3"

AES-256-CCM
test vector NIST #26 (P=24, N=7, A=32, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_256_CCM:"8c5cf3457ff22228c39c051c4e05ed4093657eb303f859a9d4b0f8be0127d88a":"6ba004fd176791":"5a053b2a1bb87e85d56527bfcdcd3ecafb991bb10e4c862bb0751c700a29f54b":"94748ba81229e53c38583a8564b23ebbafc6f6efdf4c2a81":"c44db2c9":"FAIL"

AES-256-CCM test vector NIST #27 (P=24, N=7, A=32, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_256_CCM:"705334e30f53dd2f92d190d2c1437c8772f940c55aa35e562214ed45bd458ffe":"a544218dadd3c1":"d3d5424e20fbec43ae495353ed830271515ab104f8860c988d15b6d36c038eab":"3341168eb8c48468c414347fb08f71d2086f7c2d1bd581ce":"1ac68bd42f5ec7fa7e068cc0ecd79c2a":"78c46e3249ca28e1ef0531d80fd37c124d9aecb7be6668e3"

AES-256-CCM
test vector NIST #28 (P=24, N=7, A=32, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_256_CCM:"705334e30f53dd2f92d190d2c1437c8772f940c55aa35e562214ed45bd458ffe":"6ba004fd176791":"5a053b2a1bb87e85d56527bfcdcd3ecafb991bb10e4c862bb0751c700a29f54b":"d543acda712b898cbb27b8f598b2e4438ce587a836e27851":"47c3338a2400809e739b63ba8227d2f9":"FAIL"

AES-256-CCM test vector NIST #29 (P=24, N=13, A=32, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_256_CCM:"705334e30f53dd2f92d190d2c1437c8772f940c55aa35e562214ed45bd458ffe":"a544218dadd3c10583db49cf39":"3c0e2815d37d844f7ac240ba9d6e3a0b2a86f706e885959e09a1005e024f6907":"c0ea400b599561e7905b99262b4565d5c3dc49fad84d7c69":"ef891339":"e8de970f6ee8e80ede933581b5bcf4d837e2b72baa8b00c3"

AES-256-CCM test vector NIST #30 (P=24, N=13, A=32, T=4)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_256_CCM:"705334e30f53dd2f92d190d2c1437c8772f940c55aa35e562214ed45bd458ffe":"8fa501c5dd9ac9b868144c9fa5":"5bb40e3bb72b4509324a7edc852f72535f1f6283156e63f6959ffaf39dcde800":"60871e03ea0eb968536c99f926ea24ef43d41272ad9fb7f6":"3d488623":"FAIL"

AES-256-CCM
test vector NIST #31 (P=24, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_256_CCM:"314a202f836f9f257e22d8c11757832ae5131d357a72df88f3eff0ffcee0da4e":"a544218dadd3c10583db49cf39":"3c0e2815d37d844f7ac240ba9d6e3a0b2a86f706e885959e09a1005e024f6907":"8d34cdca37ce77be68f65baf3382e31efa693e63f914a781":"367f30f2eaad8c063ca50795acd90203":"e8de970f6ee8e80ede933581b5bcf4d837e2b72baa8b00c3"

AES-256-CCM test vector NIST #32 (P=24, N=13, A=32, T=16)
depends_on:MBEDTLS_AES_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_AES_256_CCM:"314a202f836f9f257e22d8c11757832ae5131d357a72df88f3eff0ffcee0da4e":"8fa501c5dd9ac9b868144c9fa5":"5bb40e3bb72b4509324a7edc852f72535f1f6283156e63f6959ffaf3

9dcde800":"516c0095cc3d85fd55e48da17c592e0c7014b9daafb82bdc":"4b41096dfdbe9cc1ab610f8f3e038d16":"FA
IL"

Camellia-CCM
test vector RFC 5528 #1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_CAMELLIA_128_CCM:"C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF":"
00000003020100A0A1A2A3A4A5":"0001020304050607":"BA737185E719310492F38A5F1251DA55FAFBC949
848A0D":"FCAECE746B3DB9AD":"08090A0B0C0D0E0F101112131415161718191A1B1C1D1E"

Camellia-CCM test vector RFC 5528 #2
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_CAMELLIA_128_CCM:"C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF":"
00000004030201A0A1A2A3A4A5":"0001020304050607":"5D2564BF8EAFE1D99526EC016D1BF0424CFBD2C
D62848F33":"60B2295DF24283E8":"08090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F"

Camellia-CCM test vector RFC 5528 #3
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_CAMELLIA_128_CCM:"C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF":"
00000005040302A0A1A2A3A4A5":"0001020304050607":"81F663D6C7787817F9203608B982AD15DC2BBD87
D756F79204":"F551D6682F23AA46":"08090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F20"

Camellia-CCM
test vector RFC 5528 #4
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_CAMELLIA_128_CCM:"C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF":"
00000006050403A0A1A2A3A4A5":"000102030405060708090A0B":"CAEF1E827211B08F7BD90F08C77288C0
70A4A0":"8B3A933A63E497A0":"0C0D0E0F101112131415161718191A1B1C1D1E"

Camellia-CCM test vector RFC 5528 #5
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_CAMELLIA_128_CCM:"C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF":"
00000007060504A0A1A2A3A4A5":"000102030405060708090A0B":"2AD3BAD94FC52E92BE438E827C1023B
96A8A7725":"8FA17BA7F331DB09":"0C0D0E0F101112131415161718191A1B1C1D1E1F"

Camellia-CCM test vector RFC 5528 #6
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_CAMELLIA_128_CCM:"C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF":"
00000008070605A0A1A2A3A4A5":"000102030405060708090A0B":"FEA5480BA53FA8D3C34422AACE4DE6
7FFA3BB73BAB":"AB36A1EE4FE0FE28":"0C0D0E0F101112131415161718191A1B1C1D1E1F20"

Camellia-CCM
test vector RFC 5528 #7
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_CAMELLIA_128_CCM:"C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF":"
00000009080706A0A1A2A3A4A5":"0001020304050607":"54532026E54C119A8D36D9EC6E1ED97416C8708C
4B5C2C":"ACAFA3BCCF7A4EBF9573":"08090A0B0C0D0E0F101112131415161718191A1B1C1D1E"

Camellia-CCM test vector RFC 5528 #8
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_CAMELLIA_128_CCM:"C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF":"0000000A090807A0A1A2A3A4A5":"0001020304050607":"8AD19B001A87D148F4D92BEF34525CCCE3A63C6512A6F575":"7388E4913EF14701F441":"08090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F"

Camellia-CCM test vector RFC 5528 #9
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_CAMELLIA_128_CCM:"C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF":"0000000B0A0908A0A1A2A3A4A5":"0001020304050607":"5DB08D62407E6E31D60F9CA2C60474219AC0BE50C0D4A57787":"94D6E230CD25C9FEBF87":"08090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F20"

Camellia-CCM
test vector RFC 5528 #10
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_CAMELLIA_128_CCM:"C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF":"0000000C0B0A09A0A1A2A3A4A5":"000102030405060708090A0B":"DB118CCEC1B8761C877CD8963A67D6F3BBBC5C":"D09299EB11F312F23237":"0C0D0E0F101112131415161718191A1B1C1D1E"

Camellia-CCM test vector RFC 5528 #11
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_CAMELLIA_128_CCM:"C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF":"0000000D0C0B0AA0A1A2A3A4A5":"000102030405060708090A0B":"7CC83D8DC49103525B483DC5CA7EA9AB812B7056":"079DAFFADA16CCCF2C4E":"0C0D0E0F101112131415161718191A1B1C1D1E1F"

Camellia-CCM test vector RFC 5528 #12
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_CAMELLIA_128_CCM:"C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF":"0000000E0D0C0BA0A1A2A3A4A5":"000102030405060708090A0B":"2CD35B8820D23E7AA351B0E92FC79367238B2CC748":"CBB94C2947793D64AF75":"0C0D0E0F101112131415161718191A1B1C1D1E1F20"

Camellia-CCM test
vector RFC 5528 #13
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_CAMELLIA_128_CCM:"D75C2778078CA93D971F96FDE720F4CD":"00A970110E1927B160B6A31C1C":"6B7F464507FAE496":"A435D727348DDD22907F7EB8F5FDBB4D939DA6524DB4F6":"4558C02D25B127EE":"C6B5F3E6CA2311AEF7472B203E735EA561ADB17D56C5A3"

Camellia-CCM test vector RFC 5528 #14
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_CAMELLIA_128_CCM:"D75C2778078CA93D971F96FDE720F4CD":"0083CD8CE0CB42B160B6A31C1C":"986605B43DF15DE7":"8AE052508FBECA932E346F05E0DC0DFBCF939EAFFA3E587C":"867D6E1C48703806":"01F6CE6764C574483BB02E6BBF1E0ABD26A22572B4D80EE7"

Camellia-CCM test vector RFC 5528 #15
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_CAMELLIA_128_CCM:"D75C2778078CA93D971F96FDE720F4CD":"005F

54950B18F2B160B6A31C1C":"48F2E7E1A7671A51":"08B67EE21C8BF26E473E408599E9C0836D6AF0BB18DF55466C":"A80878A790476DE5":"CDF1D8406FC2E9014953897005FBFB8BA57276F92404608E08"

Camellia-CCM test
vector RFC 5528 #16
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_CAMELLIA_128_CCM:"D75C2778078CA93D971F96FDE720F4CD":"00EC600863319AB160B6A31C1C":"DE97DF3B8CBD6D8E5030DA4C":"63B78B4967B19EDBB733CD1114F64EB2260893":"68C354828D950CC5":"B005DCFA0B59181426A961685A993D8C43185B"

Camellia-CCM test vector RFC 5528 #17
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_CAMELLIA_128_CCM:"D75C2778078CA93D971F96FDE720F4CD":"0060CFF1A31EA1B160B6A31C1C":"A5EE93E457DF05466E782DCF":"0BC6BBE2A8B909F4629EE6DC148DA44410E18AF4":"3147383276F66A9F":"2E20211298105F129D5ED95B93F72D30B2FACCD7"

Camellia-CCM test vector RFC 5528 #18
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_CAMELLIA_128_CCM:"D75C2778078CA93D971F96FDE720F4CD":"000F85CD995C97B160B6A31C1C":"24AA1BF9A5CD876182A25074":"222AD632FA31D6AF970C345F7E77CA3BD0DC25B340":"A1A3D31F8D4B44B7":"2645941E75632D3491AF0FC0C9876C3BE4AA7468C9"

Camellia-CCM test vector RFC 5528 #19
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_CAMELLIA_128_CCM:"D75C2778078CA93D971F96FDE720F4CD":"00C29B2CAAC4CDB160B6A31C1C":"691946B9CA07BE87":"05B8E1B9C49CFD56CF130AA6251DC2ECC06CCC508FE697":"A0066D57C84BEC182768":"070135A6437C9DB120CD61D8F6C39C3EA125FD95A0D23D"

Camellia-CCM
test vector RFC 5528 #20
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_CAMELLIA_128_CCM:"D75C2778078CA93D971F96FDE720F4CD":"002C6B7595EE62B160B6A31C1C":"D0C54ECB84627DC4":"54CEB968DEE23611575EC003DFAA1CD48849BDF5AE2EDB6B":"7FA775B150ED4383C5A9":"C8C0880E6C636E20093DD6594217D2E18877DB264E71A5CC"

Camellia-CCM test vector RFC 5528 #21
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_CAMELLIA_128_CCM:"D75C2778078CA93D971F96FDE720F4CD":"00C53CD4C2AA24B160B6A31C1C":"E285E0E4808CDA3D":"B1404546BF667210CA28E309B39BD6CA7E9FC8285FE698D43C":"D20A02E0BDCAED2010D3":"F75DAA0710C4E64297794DC2B7D2A20757B1AA4E448002FFAB"

Camellia-CCM test vector RFC 5528
#22
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_CAMELLIA_128_CCM:"D75C2778078CA93D971F96FDE720F4CD":"00BEE9267FBADCB160B6A31C1C":"6CAEF9941141570D7C813405":"94C8959C11569A297831A721005857AB61B87A":"2DEA0936B6EB5F625F5D":"C238822FAC5F98FF929405B0AD127A4E41854E"

Camellia-CCM test vector RFC 5528 #23
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_CAMELLIA_128_CCM:"D75C2778078CA93D971F96FDE720F4CD":"00D
FA8B1245007B160B6A31C1C":"36A52CF16B19A2037AB7011E":"5869E3AAD2447C74E0FC05F9A4EA74577
F4DE8CA":"8924764296AD04119CE7":"4DBF3E774AD245E5D5891F9D1C32A0AE022C85D7"

Camellia-CCM test vector RFC 5528 #24
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CCM_C
auth_crypt_tv:MBEDTLS_CIPHER_CAMELLIA_128_CCM:"D75C2778078CA93D971F96FDE720F4CD":"003B
8FD8D3A937B160B6A31C1C":"A4D499F78419728C19178B0C":"4B198156393B0F7796086AAFB454F8C3F03
4CCA966":"945F1FCEA7E11BEE6A2F":"9DC9EDAE2FF5DF8636E8C6DE0EED55F7867E33337D"
-----BEGIN EC PRIVATE KEY-----
MIGkAgEBBDA/XY2b4oC1aWzFzJ+Uz4r35rYd1lkrKrKzpMYHRQQX7DJ9zcrtfBAF
PXGaBXTwp2qgBwYFK4EEACKhZANiAATZxmK1C6KcpHmQRQ4EOur08MabFWdtES9i
KnHJMFmvmZaRxWgNK0TREVedsS9KQTou1cRfz7Z7W2PgC5Hr5Z0JprGsLAxCgqoS
MX7VkU+Zm8SIuxMug0LMNvLKXjN5x0c=
-----END EC PRIVATE KEY-----
add_executable(gen_random_havege gen_random_havege.c)
target_link_libraries(gen_random_havege mbedtls)

add_executable(gen_random_ctr_drbg gen_random_ctr_drbg.c)
target_link_libraries(gen_random_ctr_drbg mbedtls)

add_executable(gen_entropy gen_entropy.c)
target_link_libraries(gen_entropy mbedtls)

install(TARGETS gen_random_havege gen_random_ctr_drbg gen_entropy
    DESTINATION "bin"
    PERMISSIONS OWNER_READ OWNER_WRITE OWNER_EXECUTE GROUP_READ
GROUP_EXECUTE WORLD_READ WORLD_EXECUTE)
-----BEGIN CERTIFICATE-----
MIIDpzCCAo+gAwIBAgIBITANBgkqhkiG9w0BAQsFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTQwNDAxMTQ0NDQzWhcNMjQwMzI5MTQ0NDQzWjA8MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxGjAYBgNVBAMTEVBvbGFyU1NMIFNlcnZlciAxMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqQIfPUBq1VVTi/027oJlLhVhXom/
uOhFkNvuiBZS0/FDUEeWEllkh2v9K+BG+XO+3c+S4ZFb7Wagb4kpeUWA0INq1UFD
d185fAkER4KwVzlw7aPsFRkeqDMIR8EFQqn9TMO0390GH00QUUBncxMPQPhtgSVf
CrFTxjB+FTms+Vruf5KepgVb5xOXhbUjktnUJAbVCSWJdQfdphqPPwkZvq1lLGTr
lZvc/kFeF6babFtpzAK6FCwWJJxK3M3Q91Jnc/EtoCP9fvQxyi1wyokLBNsupk9w
bp7OvViJ4lNZnm5akmXiiD8MlBmj3eXonZUT7Snbq3AS3FrKaxerUoJUsQIDAQAB
o4G0MIGxMAkGA1UdEwQCMAAwHQYDVR0OBBYEFB901j8pwXR0RTsFEiw9qL1DWQKm
MGMGA1UdIwRcMFqAFLRa5KWz3tJS9rnVppUP6z68x/3/oT+kPTA7MQswCQYDVQQG
EwJOTDERMA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3Qg
Q0GCAQAwCwYDVR0PBAQDAgXgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCSqGSIb3
DQEBCwUAA4IBAQANtiYR2P6+a7rEtJARIgpurw1URYejATbbp3ZhaHBW603Wyb2+
KJtm1KPCzoju/qTRt65YYkt+tu1wTzamyrkPxt8bBKmxiWnu5j1HLxdjOz8VW9lf

vTb5egR4dU9eNXni/5QkzrdkMO+ob4puDXY7ytPuGX6YfNVhCkrhBlYDJNE57CkK
vpCNj3+Te8PEkWPAEaUhqCnQk6qvPvpBfc/hqgwzlRMt3u5NkiVOuH72dtr4fOI1
nlAU8D2wuvDVr3X5281ONNEtHU6rXe98vlUzS9QV9lBDdsO9nRYJzv2Nb1cjRIM5
JZl0ILLR2tc6E/W5YXalNp37jfrFii1U9WrJ
-----END
CERTIFICATE-----
-----BEGIN X509 CRL-----
MIIBqzCBlDANBgkqhkiG9w0BAQQFADA7MQswCQYDVQQGEwJOTDERMA8GA1UEChMI
UG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EXDTExMDIxMjE0NDQw
N1oXDTExMDQxMzE0NDQwN1owKDASAgEBFw0xMTAyMTIxNDQ0MDdaMBICAQMXDTEx
MDIxMjE0NDQwN1owDQYJKoZIhvcNAQEEBQADggEBAKKCJZ1MwL+gKAw3RV4qEmb9
gMDdSLJ1Vdkn9FgDx2ijNnYDtvaW+I3sOXrq7O6gVN1KEamJJbufVJA5+OE2oVbC
husEdgQm8D5TbrGcjPIPWxgYyuuRsl7XovZhXnqTIUrC+J8oH9XzKaMc+HZb5UhR
h8bzcyp+9jbBje7lWwKTzkuvd/I7VbS02TUkWFJTrYB0Laj8WMcgcZiyX0iZuj8j
4hOupu0lPoSzZ4h7t0Vmay6wO+8n8LJohyiwYS7LddpOjIdP0MWifN7u/ArqNNlh
2kg8eAc1pYOU/pJFTAAbOmC/kQpa9skd+PPIPPh9T53o3yeDQA0vFqN92JryCCU=
-----END X509 CRL-----
'|'DW~J>UN*X"Qdi!q4],0V)oj~mGwP j$
N4F>5/41z|-
h*hA~
f0-/b2
-----BEGIN CERTIFICATE-----
MIIDijCCAnKgAwIBAgIBMDANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTQwNDA5MTAwMjQ5WhcNMjQwNDA2MTAwMjQ5WjA0MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxEjAQBgNVBAMTCWxvY2FsaG9zdDCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBAMFNo93nzR3RBNdJcriZrA545Do8Ss86ExbQWuTN
owCIp+4ea5anUrSQ7y1yej4kmvy2NKwk9XfgJmSMnLAofaHa6ozmyRyWvP7BBFKz
NtSj+uGxdtiQwWG0ZlI2oiZTqqt0Xgd9GYLbKtgfoNkNHC1JZvdbJXNG6AuKT2kM
tQCQ4dqCEGZ9rlQri2V5kaHiYcPNQEkI7mgM8YuG0ka/0LiqEQMef1aoGh5EGA8P
hYvai0Re4hjGYi/HZo36Xdh98yeJKQHFkA4/J/EwyEoO79bex8cna8cFPXrEAjya
HT4P6DSYW8tzS1KW2BGiLICIaTla0w+w3lkvEcf36hIBMJcCAwEAAaOBnzCBnDAJ
BgNVHRMEAjAAMB0GA1UdDgQWBBSlBehkuNzfYA9QEk1gqGSvTYtDkzBjBgNVHSME
XDBagBS0WuSls97SUva51aaVD+s+vMf9/6E/pD0wOzELMAkGA1UEBhMCTkwxETAP
BgNVBAoTCFBvbGFyU1NMMRkwFwYDVQQDExBQb2xhclNTTCBUZXN0IENBggEAMAsG
A1UdDwQEAwIFoDANBgkqhkiG9w0BAQUFAAOCAQEAnW7+h85xBP2KJzFSpWfGirVe
ApdC9bX0Z1sVMmD486N+ty9W6BP6kJRxLDX0fOuRc3x7mCy5qZg/Yj40+yQSoA0w
bTNwJjuR8iMqWIqLw9hWR+E9T4lYLZWyGJVjlVTkO4i5wifwhoJE9Doohh/6crn5
ImWgEkgT/wDVIHoamciO6KU36d0iAEEP2eYgxv2/sVHvjjsseTdvYh3D3VuOmQtS
uUvFxc6H5kYoq/yodJWDaOn3RS8pEpDsiW+abcWyxNTPtHFroJV7e9aaVmhlRSzw
sYDyD/ZyIlavoPSEiD3LTT/Tp6BIpz+zb4WHOHLEvUCsZputqxPVcNoEAi9xuA==
-----END
CERTIFICATE-----
[req]
x509_extensions = v3_ca
distinguished_name = req_dn

[req_dn]

countryName = NL
organizationalUnitName = PolarSSL
commonName = PolarSSL Test CA

[v3_ca]
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid:always,issuer:always
basicConstraints = CA:true
-----BEGIN CERTIFICATE-----
MIIB/TCCAYCgAwIBAgIBATAMBggqhkjOPQQDAgUAMD4xCzAJBgNVBAYTAk5MMREw
DwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBFQyBDQTAe
Fw0wMzA5MjQxNTQ5NDhaFw0xMzA5MjQxNTQ5NDhaMD4xCzAJBgNVBAYTAk5MMREw
DwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBFQyBDQTB2
MBAGByqGSM49AgEGBSuBBAAiA2IABMPaKzRBN1gvh1b+/Im6KUNLTuBuww5XUzM5
WNRStJGVOQsj318XJGJI/BqVKc4sLYfCiFKAr9ZqqyHduNMcbli4yuiyaY7zQa0p
w7RfdadHb9UZKVVpmlM7ILRmFmAzHqNQME4wDAYDVR0TBAUwAwEB/zAdBgNVHQ4E
FgQUnW0gJEkBPyvLeLUZvH4kydv7NnwwHwYDVR0jBBgwFoAUnW0gJEkBPyvLeLUZ
vH4kydv7NnwwDAYIKoZIzj0EAwIFAANpADBmAjEAvQ/49lXXrLYdOIGtTaYWjpZP
tRBXQiGPMzUvmKBk7gM7bF4iFPsdJikyXHmuwv3RAjEA8vtUX8fAAB3fbh5dEXRm
l7tz0Sw/RW6AHFtaIauGkhHqeKIaKIi6WSgHu6x97uyg
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIICIDCCAaWgAwIBAgIBCjAKBggqhkjOPQQDAjA+MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EwHhcN
MTMwOTI0MTU1MjA0WhcNMjMwOTIyMTU1MjA0WjA0MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxEjAQBgNVBAMTCWxvY2FsaG9zdDBZMBMGByqGSM49AgEG
CCqGSM49AwEHA0IABIFZMXZJJPoVraugMW4O7TMR+pElVcGwwZwDcj6Yui2kcjeJ
H0M3jR+OOtjwV+gvT8kApPfbcw+yxgSU0UA7OOOjgZ0wgZowCQYDVR0TBAIwADAd
BgNVHQ4EFgQUfmWPPjMDFOXhvmCy4IV/jOdgK3swbgYDVR0jBGcwZYAUnW0gJEkB
PyvLeLUZvH4kydv7NnyhQqRAMD4xCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQb2xh
clNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBFQyBDQYIJAMFD4n5iQ8zoMAoG
CCqGSM49BAMCA2kAMGYCMQCsYTyleBFuI4nizuxo/ie5dxJnD0ynwCnRJ+84PZP4
AQA3HdUz0qNYs4CZ2am9Gz0CMQDr2TNLFA3C3S3pmgXMT0eKzR1Ca1/Nulf0llQZ
Xj09kLboxuemP40IIqhQnpYptMg=
-----END
CERTIFICATE-----
Memory buffer alloc self test
mbedtls_memory_buffer_alloc_self_test:

Memory buffer alloc - free in middle, alloc at end
memory_buffer_alloc_free_alloc:100:100:100:0:0:1:0:0:200:0

Memory buffer alloc - free in middle, realloc
memory_buffer_alloc_free_alloc:100:100:100:0:0:1:0:0:100:0

Memory buffer alloc - free in middle, merge, realloc
memory_buffer_alloc_free_alloc:100:100:100:100:0:1:1:0:201:0

Memory buffer alloc - free at end, merge, realloc
memory_buffer_alloc_free_alloc:100:64:100:100:0:0:0:1:200:0

Memory buffer alloc - Out of Memory test
memory_buffer_alloc_oom_test:

```
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
   <Configuration>Release</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\ssl\dtls_client.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">

   <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid>{FE7AB78F-DBF1-0721-3522-0D7C3011D2E5}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>dtls_client</RootNamespace>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
```

```
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
/>
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
```

```
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
   <PrecompiledHeader>
   </PrecompiledHeader>
   <WarningLevel>Level3</WarningLevel>
   <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
    <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
   <SubSystem>Console</SubSystem>
   <GenerateDebugInformation>true</GenerateDebugInformation>
   <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
   <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
   <PrecompiledHeader>
   </PrecompiledHeader>
   <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
 <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
   <SubSystem>Console</SubSystem>
   <GenerateDebugInformation>true</GenerateDebugInformation>
   <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
   <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
```

```
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
  </Link>
 </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
 <Import
 Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
```

```
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
   <Configuration>Release</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\aes\aescrypt2.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">

  <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid>{7A851DBD-7D57-E8F4-85E5-CCA72AEA7DF8}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>aescrypt2</RootNamespace>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
```

```
    <ConfigurationType>Application</ConfigurationType>
    <UseDebugLibraries>false</UseDebugLibraries>
    <WholeProgramOptimization>true</WholeProgramOptimization>
    <CharacterSet>Unicode</CharacterSet>
  </PropertyGroup>
  <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
    <ConfigurationType>Application</ConfigurationType>
    <UseDebugLibraries>false</UseDebugLibraries>
    <WholeProgramOptimization>true</WholeProgramOptimization>
    <CharacterSet>Unicode</CharacterSet>
    <PlatformToolset>Windows7.1SDK</PlatformToolset>
  </PropertyGroup>
  <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
  <ImportGroup Label="ExtensionSettings">
  </ImportGroup>
  <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
    <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
  />
  </ImportGroup>
  <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
    <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
  </ImportGroup>
  <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
    <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
  </ImportGroup>
  <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
    <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
  </ImportGroup>
  <PropertyGroup Label="UserMacros" />
  <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
     <LinkIncremental>true</LinkIncremental>
    <IntDir>$(Configuration)\$(TargetName)\</IntDir>
  </PropertyGroup>
  <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
    <LinkIncremental>true</LinkIncremental>
    <IntDir>$(Configuration)\$(TargetName)\</IntDir>
  </PropertyGroup>
  <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
    <LinkIncremental>false</LinkIncremental>
    <IntDir>$(Configuration)\$(TargetName)\</IntDir>
  </PropertyGroup>
  <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
    <LinkIncremental>false</LinkIncremental>
    <IntDir>$(Configuration)\$(TargetName)\</IntDir>
```

```
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
     <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
 <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
```

```
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
  </Link>
 </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
 <Import
 Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
set(THREADS_USE_PTHREADS_WIN32 true)
find_package(Threads)

set(libs
```

```
  mbedtls
)

set(targets
  dtls_client
  dtls_server
  ssl_client1
  ssl_client2
  ssl_server
  ssl_fork_server
  ssl_mail_client
  mini_client
)

if(USE_PKCS11_HELPER_LIBRARY)
  set(libs ${libs} pkcs11-helper)
endif(USE_PKCS11_HELPER_LIBRARY)

if(ENABLE_ZLIB_SUPPORT)
  set(libs ${libs} ${ZLIB_LIBRARIES})
endif(ENABLE_ZLIB_SUPPORT)

add_executable(dtls_client dtls_client.c)
target_link_libraries(dtls_client ${libs})

add_executable(dtls_server dtls_server.c)
target_link_libraries(dtls_server ${libs})

add_executable(ssl_client1 ssl_client1.c)
target_link_libraries(ssl_client1 ${libs})

add_executable(ssl_client2 ssl_client2.c)
target_link_libraries(ssl_client2 ${libs})

add_executable(ssl_server ssl_server.c)
target_link_libraries(ssl_server ${libs})

add_executable(ssl_server2 ssl_server2.c)
target_link_libraries(ssl_server2 ${libs})

add_executable(ssl_fork_server ssl_fork_server.c)
target_link_libraries(ssl_fork_server
 ${libs})

add_executable(ssl_mail_client ssl_mail_client.c)
target_link_libraries(ssl_mail_client ${libs})

add_executable(mini_client mini_client.c)
```

```
target_link_libraries(mini_client ${libs})

if(THREADS_FOUND)
  add_executable(ssl_pthread_server ssl_pthread_server.c)
  target_link_libraries(ssl_pthread_server ${libs} ${CMAKE_THREAD_LIBS_INIT})
  set(targets ${targets} ssl_pthread_server)
endif(THREADS_FOUND)

install(TARGETS ${targets}
      DESTINATION "bin"
      PERMISSIONS OWNER_READ OWNER_WRITE OWNER_EXECUTE GROUP_READ
GROUP_EXECUTE WORLD_READ WORLD_EXECUTE)
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIPEqEyB2AnCoPL/9U/YDHvdqXYbIogTywwyp6/UfDw6noAoGCCqGSM49
AwEHoUQDQgAEN8xW2XYJHlpyPsdZLf8gbu58+QaRdNCtFLX3aCJZYpJO5QDYIxH/
6i/SNF1dFr2KiMJrdw1VzYoqDvoByLTt/w==
-----END EC PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIBWjCCAQCgAwIBAgIBSzAKBggqhkjOPQQDAjBKMQswCQYDVQQGEwJVSzERMA8G
A1UEChMIbWJlZCBUTFMxKDAmBgNVBAMTH21iZWQgVExTIFRlc3QgaW50ZXJtZWRp
YXRlIENBIDMwHhcNMTUwOTAxMTM0NzU1WhcNMjUwODI5MTM0NzU1WjAUMRIwEAYD
VQQDEwlsb2NhbGhvc3QwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQcbffp2qXq
oZyychmoCRxzrd4Vu96m47NPBehtEC46aTeXgDnBdf++znABrAtfXBRNQz8ARIeY
Bmskr22rlKjyow0wCzAJBgNVHRMEAjAAMAoGCCqGSM49BAMCA0gAMEUCIQDLc+Io
rg8VxEbCgVv8iH+kOIEn9MjhpvKzvwUoV+6rjQIgZU/RXAyc1a+H2+soGfNEIOBQ
AzO3pJx7WJAApZuBX1Q=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIBwjCCAUegAwIBAgIBSTAKBggqhkjOPQQDAjBLMQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxKTAnBgNVBAMTIFBvbGFyU1NMIFRlc3QgSW50ZXJtZWRp
YXRlIEVDIENBMB4XDTE1MDkwMTEzNDIxOFoXDTI1MDgyOTEzNDIxOFowSjELMAkG
A1UEBhMCVUsxETAPBgNVBAoTCG1iZWQgVExTMSgwJgYDVQQDEx9tYmVkIFRMUyBU
ZXN0IGludGVybWVkaWF0ZSBDQSAzMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE
732fWHLNPMPsP1U1ibXvb55erlEVMlpXBGsj+KYwVqU1XCmW9Z9hhP7X/5js/DX9
2J/utoHyjUtVpQOzdTrbsaMdMBswDAYDVR0TBAUwAwEB/zALBgNVHQ8EBAMCB4Aw
CgYIKoZIzj0EAwIDaQAwZgIxAJ9RX38bht+RNsQI2GUpNhC/Y+Tb1OU74O4iEa6+
CkjBWTpLtHRKVdZq7ST0wk1LsQIxAIUi8L1Vx4DuUP0bJxIX/nuJqlBnBG+qRhSf
VgHKgSyHidpZAJpaRi4IkY504CY/Yg==
-----END
 CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIC6TCCAdGgAwIBAgIBDzANBgkqhkiG9w0BAQsFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTMwOTI0MTYwODQyWhcNMjMwOTIyMTYwODQyWjBLMQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxKTAnBgNVBAMTIFBvbGFyU1NMIFRlc3QgSW50ZXJtZWRp
YXRlIEVDIENBMHYwEAYHKoZIzj0CAQYFK4EEACIDYgAE8Oih3fX5SLeN1dmFncQl
WMw9+Y6sXblhlrXBxhXxjwdwpCHENn+foUVdrqYVYa7Suv3QVeO6nJ19H3QNixW8
ik1P+hxsbaq8bta78vAyHmC4EmXQLg1w7oxb9Q82qX1Yo4GVMIGSMB0GA1UdDgQW
```

BBQPib1jQevLXhco/2gwPcGI0JxYOTBjBgNVHSMEXDBagBS0WuSls97SUva51aaV
D+s+vMf9/6E/pD0wOzELMAkGA1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NMMRkw
FwYDVQQDExBQb2xhclNTTCBUZXN0IENBggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZI
hvcNAQELBQADggEBAAjeaTUaCBiXT1CYLVr6UFSeRNZBrDPnj6PwqUQTvgB5I5n6
yXqoE4RYDaEL0Lg24juFxI26itBuypto6vscgGq77cfrP/avSdxU+xeZ4bCWvh3M
ddj9lmko2U8I8GhBcHpSuIiTvgKDB8eKkjeq3AsLGchHDvip8pB3IhcNfL7W94Zf
7/lH9VQiE3/px7amD32cidoPvWLA9U3f1FsPmJESUz0wwNfINpDjmPr8dGbkCN+M
CFhxo6sCfK8KLYG4nYX8FwxVR86kpSrO9e84AX0YYbdzxprbc2XOaebJ8+BDmzut
ARkD7DTXrodN1wV7jQJkrUuEwPj9Rhvk+MFRkaw=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIBWjCCAQCgAwIBAgIBSzAKBggqhkjOPQQDAjBKMQswCQYDVQQGEwJVSzERMA8G
A1UEChMIbWJlZCBUTFMxKDAmBgNVBAMTH21iZWQgVExTIFRlc3QgaW50ZXJtZWRp
YXRlIENBIDMwHhcNMTUwOTAxMTM0NzU1WhcNMjUwODI5MTM0NzU1WjAUMRIwEAYD
VQQDEwlsb2NhbGhvc3QwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQcbffp2qXq
oZyychmoCRxzrd4Vu96m47NPBehtEC46aTeXgDnBdf++znABrAtfXBRNQz8ARIeY
Bmskr22rlKjyow0wCzAJBgNVHRMEAjAAMAoGCCqGSM49BAMCA0gAMEUCIQDLc+Io
rg8VxEbCgVv8iH+kOIEn9MjhpvKzvwUoV+6rjQIgZU/RXAyc1a+H2+soGfNEIOBQ
AzO3pJx7WJAApZuBX1Q=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIBtDCCATqgAwIBAgIBTTAKBggqhkjOPQQDAjBLMQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxKTAnBgNVBAMTIFBvbGFyU1NMIFRlc3QgSW50ZXJtZWRp
YXRlIEVDIENBMB4XDTE1MDkwMTE0MDg0M1oXDTI1MDgyOTE0MDg0M1owSjELMAkG
A1UEBhMCVUsxETAPBgNVBAoTCG1iZWQgVExTMSgwJgYDVQQDEx9tYmVkIFRMUyBU
ZXN0IGludGVybWVkaWF0ZSBDQSAzMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE
732fWHLNPMPsP1U1ibXvb55erlEVMlpXBGsj+KYwVqU1XCmW9Z9hhP7X/5js/DX9
2J/utoHyjUtVpQOzdTrbsaMQMA4wDAYDVR0TBAUwAwEB/zAKBggqhkjOPQQDAgNo
ADBlAjAJRxbGRas3NBmk9MnGWXg7PT1xnRELHRWWIvfLdVQt06l1/xFg3ZuPdQdt
Qh7CK80CMQD7wa1o1a8qyDKBfLN636uKmKGga0E+vYXBeFCy9oARBangGCB0B2vt
pz590JvGWfM=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIC6TCCAdGgAwIBAgIBDzANBgkqhkiG9w0BAQsFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTMwOTI0MTYwODQyWhcNMjMwOTIyMTYwODQyWjBLMQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxKTAnBgNVBAMTIFBvbGFyU1NMIFRlc3QgSW50ZXJtZWRp
YXRlIEVDIENBMHYwEAYHKoZIzj0CAQYFK4EEACIDYgAE8Oih3fX5SLeN1dmFncQl
WMw9+Y6sXblhlrXBxhXxjwdwpCHENn+foUVdrqYVYa7Suv3QVeO6nJ19H3QNixW8
ik1P+hxsbaq8bta78vAyHmC4EmXQLg1w7oxb9Q82qX1Yo4GVMIGSMB0GA1UdDgQW
BBQPib1jQevLXhco/2gwPcGI0JxYOTBjBgNVHSMEXDBagBS0WuSls97SUva51aaV
D+s+vMf9/6E/pD0wOzELMAkGA1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NMMRkw
FwYDVQQDExBQb2xhclNTTCBUZXN0IENBggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZI
hvcNAQELBQADggEBAAjeaTUaCBiXT1CYLVr6UFSeRNZBrDPnj6PwqUQTvgB5I5n6
yXqoE4RYDaEL0Lg24juFxI26itBuypto6vscgGq77cfrP/avSdxU+xeZ4bCWvh3M
ddj9lmko2U8I8GhBcHpSuIiTvgKDB8eKkjeq3AsLGchHDvip8pB3IhcNfL7W94Zf

```
7/lH9VQiE3/px7amD32cidoPvWLA9U3f1FsPmJESUz0wwNfINpDjmPr8dGbkCN+M
CFhxo6sCfK8KLYG4nYX8FwxVR86kpSrO9e84AX0YYbdzxprbc2XOaebJ8+BDmzut
ARkD7DTXrodN1wV7jQJkrUuEwPj9Rhvk+MFRkaw=
-----END
 CERTIFICATE-----
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 0 (0x0)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=NL, O=PolarSSL, CN=PolarSSL Test CA
    Validity
      Not Before: Feb 12 14:44:00 2011 GMT
      Not After : Feb 12 14:44:00 2021 GMT
    Subject: C=NL, O=PolarSSL, CN=PolarSSL Test CA
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (2048 bit)

        Modulus (2048 bit):
            00:c0:df:37:fc:17:bb:e0:96:9d:3f:86:de:96:32:
            7d:44:a5:16:a0:cd:21:f1:99:d4:ec:ea:cb:7c:18:
            58:08:94:a5:ec:9b:c5:8b:df:1a:1e:99:38:99:87:
            1e:7b:c0:8d:39:df:38:5d:70:78:07:d3:9e:d9:93:
            e8:b9:72:51:c5:ce:a3:30:52:a9:f2:e7:40:70:14:
            cb:44:a2:72:0b:c2:e5:40:f9:3e:e5:a6:0e:b3:f9:
            ec:4a:63:c0:b8:29:00:74:9c:57:3b:a8:a5:04:90:
            71:f1:bd:83:d9:3f:d6:a5:e2:3c:2a:8f:ef:27:60:
            c3:c6:9f:cb:ba:ec:60:7d:b7:e6:84:32:be:4f:fb:
            58:26:22:03:5b:d4:b4:d5:fb:f5:e3:96:2e:70:c0:
            e4:2e:bd:fc:2e:ee:e2:41:55:c0:34:2e:7d:24:72:
            69:cb:47:b1:14:40:83:7d:67:f4:86:f6:31:ab:f1:
            79:a4:b2:b5:2e:12:f9:84:17:f0:62:6f:27:3e:13:
            58:b1:54:0d:21:9a:73:37:a1:30:cf:6f:92:dc:f6:
            e9:fc:ac:db:2e:28:d1:7e:02:4b:23:a0:15:f2:38:
             65:64:09:ea:0c:6e:8e:1b:17:a0:71:c8:b3:9b:c9:
            ab:e9:c3:f2:cf:87:96:8f:80:02:32:9e:99:58:6f:
            a2:d5
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints:
        CA:TRUE
      X509v3 Subject Key Identifier:
        B4:5A:E4:A5:B3:DE:D2:52:F6:B9:D5:A6:95:0F:EB:3E:BC:C7:FD:FF
      X509v3 Authority Key Identifier:
        keyid:B4:5A:E4:A5:B3:DE:D2:52:F6:B9:D5:A6:95:0F:EB:3E:BC:C7:FD:FF
        DirName:/C=NL/O=PolarSSL/CN=PolarSSL Test CA
        serial:00
```

```
  Signature Algorithm: sha1WithRSAEncryption
      b8:fd:54:d8:00:54:90:8b:25:b0:27:dd:95:cd:a2:f7:84:07:
      1d:87:89:4a:c4:78:11:d8:07:b5:d7:22:50:8e:48:eb:62:7a:
      32:89:be:63:47:53:ff:b6:be:f1:2e:8c:54:c0:99:3f:a0:b9:
      37:23:72:5f:0d:46:59:8f:d8:47:cd:97:4c:9f:07:0c:12:62:
      09:3a:24:e4:36:d9:e9:2c:da:38:d0:73:75:61:d7:c1:6c:26:
       8b:9b:e0:d5:dc:67:ed:8c:6b:33:d7:74:22:3c:4c:db:b5:8d:
      2a:ce:2c:0d:08:59:05:09:05:a6:39:9f:b3:67:1b:e2:83:e5:
      e1:8f:53:f6:67:93:c7:f9:6f:76:44:58:12:e8:3a:d4:97:e7:
      e9:c0:3e:a8:7a:72:3d:87:53:1f:e5:2c:84:84:e7:9a:9e:7f:
      66:d9:1f:9b:f5:13:48:b0:4d:14:d1:de:b2:24:d9:78:7d:f5:
      35:cc:58:19:d1:d2:99:ef:4d:73:f8:1f:89:d4:5a:d0:52:ce:
      09:f5:b1:46:51:6a:00:8e:3b:cc:6f:63:01:00:99:ed:9d:a6:
      08:60:cd:32:18:d0:73:e0:58:71:d9:e5:d2:53:d7:8d:d0:ca:
      e9:5d:2a:0a:0d:5d:55:ec:21:50:17:16:e6:06:4a:cd:5e:de:
      f7:e0:e9:54
-----BEGIN CERTIFICATE-----
MIIDhzCCAm+gAwIBAgIBADANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTEwMjEyMTQ0NDAwWhcNMjEwMjEyMTQ0NDAwWjA7MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDA3zf8F7vglp0/ht6WMn1EpRagzSHx
mdTs6st8GFgIlKXsm8WL3xoemTiZhx57wI053zhdcHgH057Zk+i5clHFzqMwUqny
50BwFMtEonILwuVA+T7lpg6z+exKY8C4KQB0nFc7qKUEkHHxvYPZP9al4jwqj+8n
YMPGn8u67GB9t+aEMr5P+1gmIgNb1LTV+/Xjli5wwOQuvfwu7uJBVcA0Ln0kcmnL
R7EUQIN9Z/SG9jGr8XmksrUuEvmEF/Bibyc+E1ixVA0hmnM3oTDPb5Lc9un8rNsu
KNF+AksjoBXyOGVkCeoMbo4bF6BxyLObyavpw/LPh5aPgAIynplYb6LVAgMBAAGj
gZUwgZIwDAYDVR0TBAUwAwEB/zAdBgNVHQ4EFgQUtFrkpbPe0lL2udWmlQ/rPrzH
/f8wYwYDVR0jBFwwWoAUtFrkpbPe0lL2udWmlQ/rPrzH/f+hP6Q9MDsxCzAJBgNV
BAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEZMBcGA1UEAxMQUG9sYXJTU0wgVGVz
dCBDQYIBADANBgkqhkiG9w0BAQUFAAOCAQEAuP1U2ABUkIslsCfdlc2i94QHHYeJ
SsR4EdgHtdciUI5I62J6Mom+Y0dT/7a+8S6MVMCZP6C5NyNyXw1GWY/YR82XTJ8H
DBJiCTok5DbZ6SzaONBzdWHXwWwmi5vg1dxn7YxrM9d0IjxM27WNKs4sDQhZBQkF
pjmfs2cb4oPl4Y9T9meTx/lvdkRYEug61Jfn6cA+qHpyPYdTH+UshITnmp5/Ztkf
m/UTSLBNFNHesiTZeH31NcxYGdHSme9Nc/gfidRa0FLOCfWxRlFqAI47zG9jAQCZ
7Z2mCGDNMhjQc+BYcdnl0lPXjdDK6V0qCg1dVewhUBcW5gZKzV7e9+DpVA==
-----END
 CERTIFICATE-----
-----BEGIN X509 CRL-----
MIICJDCCAQYCAQEwEwYJKoZIhvcNAQEKMAaiBAICAOowOzELMAkGA1UEBhMCTkwx
ETAPBgNVBAoTCFBvbGFyU1NMMRkwFwYDVQQDExBQb2xhclNTTCBUZXN0IENBFw0x
NDAxMjAxMzQ2MzVaFw0yNDAxMTgxMzQ2MzVaMCgwEgIBChcNMTMwOTI0MTYyODM4
WjASAgEWFw0xNDAxMjAxMzQzMDVaoGcwZTBjBgNVHSMEXDBagBS0WuSls97SUva5
1aaVD+s+vMf9/6E/pD0wOzELMAkGA1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NM
MRkwFwYDVQQDExBQb2xhclNTTCBUZXN0IENBggEAMBMGCSqGSIb3DQEBCjAGogQC
AgDqA4IBAQB8ZBX0BEgRcx0lfk1ctELRu1AYoJ5BnsmQpq23Ca4YIP2yb2kTN1ZS
4fR4SgYcNctgo2JJiNiUkCu1ZnRUOJUy8UlEio0+aeumTNz6CbeJEDhr5NC3oiV0
```

```
MzvLn9rJVLPetOT9UrvvIy8iz5Pn1d8mu5rkt9BKQRq9NQx8riKnSIoTc91NLCMo
mkCCB55DVbazODSWK19e6yQ0JS454RglOsqRtLJ/EDbi6lCsLXotFt3GEGMrob1O
7Qck1Z59boaHxGYFEVnx90+4M3/qikVtwZdcBjLEmfuwYvszFw8J2y6Xwmg/HtUa
y6li0JzWNHtkKUlCv2+SESZbD3NU8GQY
-----END X509 CRL-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIPb3hmTxZ3/mZI3vyk7p3U3wBf+WIop6hDhkFzJhmLcqoAoGCCqGSM49
AwEHoUQDQgAEV+WusXPf06y7k7iB/xKu7uZTrM5VU/Y0Dswu42MlC9+Y4vNcYDaW
wNUYFHDlf5/VS0UY5bBs1Vz4lo+HcKPkxw==
-----END EC PRIVATE KEY-----
cmake_minimum_required(VERSION 2.6)
project("mbed TLS" C)

option(USE_PKCS11_HELPER_LIBRARY "Build mbed TLS with the pkcs11-helper library." OFF)
option(ENABLE_ZLIB_SUPPORT "Build mbed TLS with zlib library." OFF)

option(ENABLE_PROGRAMS "Build mbed TLS programs." ON)

option(UNSAFE_BUILD "Allow unsafe builds. These builds ARE NOT SECURE." OFF)

# the test suites currently have compile errors with MSVC
if(MSVC)
  option(ENABLE_TESTING "Build mbed TLS tests." OFF)
else()
  option(ENABLE_TESTING "Build mbed TLS tests." ON)
endif()

# Warning string - created as a list for compatibility with CMake 2.8
set(WARNING_BORDER "*************************************************************\n")
set(NULL_ENTROPY_WARN_L1 "****  WARNING!  MBEDTLS_TEST_NULL_ENTROPY defined!\n")
set(NULL_ENTROPY_WARN_L2 "****  THIS BUILD HAS NO DEFINED ENTROPY SOURCES\n")
set(NULL_ENTROPY_WARN_L3 "****  AND IS *NOT* SUITABLE FOR PRODUCTION USE\n")

set(NULL_ENTROPY_WARNING "${WARNING_BORDER}"
                         "${NULL_ENTROPY_WARN_L1}"
                          "${NULL_ENTROPY_WARN_L2}"
                         "${NULL_ENTROPY_WARN_L3}"
                         "${WARNING_BORDER}")

find_package(Perl)
if(PERL_FOUND)

  # If NULL Entropy is configured, display an appropriate warning
  execute_process(COMMAND ${PERL_EXECUTABLE} ${CMAKE_SOURCE_DIR}/scripts/config.pl -f
${CMAKE_SOURCE_DIR}/include/mbedtls/config.h get MBEDTLS_TEST_NULL_ENTROPY
                  RESULT_VARIABLE result)
  if(${result} EQUAL 0)
     message(WARNING ${NULL_ENTROPY_WARNING})
```

```
      if(NOT UNSAFE_BUILD)
         message(FATAL_ERROR "\
\n\
Warning! You have enabled MBEDTLS_TEST_NULL_ENTROPY. \
This option is not safe for production use and negates all security \
It is intended for development use only. \
\n\
To confirm you want to build with this option, re-run cmake with the \
option: \n\
 cmake -DUNSAFE_BUILD=ON ")

         return()
      endif()
   endif()
endif()

set(CMAKE_BUILD_TYPE ${CMAKE_BUILD_TYPE}
    CACHE STRING "Choose the type of build: None Debug Release Coverage ASan ASanDbg MemSan
MemSanDbg Check CheckFull"
   FORCE)

string(REGEX MATCH "Clang" CMAKE_COMPILER_IS_CLANG "${CMAKE_C_COMPILER_ID}")

if(CMAKE_COMPILER_IS_GNUCC)
   # some warnings we want are not available with old GCC versions
   # note: starting with CMake 2.8 we could use CMAKE_C_COMPILER_VERSION
   execute_process(COMMAND ${CMAKE_C_COMPILER} -dumpversion
                   OUTPUT_VARIABLE GCC_VERSION)
   set(CMAKE_C_FLAGS "${CMAKE_C_FLAGS} -Wall -Wextra -W -Wdeclaration-after-statement -Wwrite-
strings")
   if (GCC_VERSION VERSION_GREATER 4.5 OR GCC_VERSION VERSION_EQUAL 4.5)
      set(CMAKE_C_FLAGS "${CMAKE_C_FLAGS} -Wlogical-op")
   endif()
   if (GCC_VERSION VERSION_GREATER 4.8 OR GCC_VERSION VERSION_EQUAL 4.8)
      set(CMAKE_C_FLAGS "${CMAKE_C_FLAGS} -Wshadow")
   endif()
   set(CMAKE_C_FLAGS_RELEASE     "-O2")
   set(CMAKE_C_FLAGS_DEBUG       "-O0 -g3")
   set(CMAKE_C_FLAGS_COVERAGE
    "-O0 -g3 --coverage")
   set(CMAKE_C_FLAGS_ASAN        "-Werror -fsanitize=address -fno-common -O3")
   set(CMAKE_C_FLAGS_ASANDBG     "-Werror -fsanitize=address -fno-common -O1 -g3 -fno-omit-frame-
pointer -fno-optimize-sibling-calls ")
   set(CMAKE_C_FLAGS_CHECK       "-Werror -Os")
   set(CMAKE_C_FLAGS_CHECKFULL   "${CMAKE_C_FLAGS_CHECK} -Wcast-qual")
endif(CMAKE_COMPILER_IS_GNUCC)
```

```
if(CMAKE_COMPILER_IS_CLANG)
  set(CMAKE_C_FLAGS "${CMAKE_C_FLAGS} -Wall -Wextra -W -Wdeclaration-after-statement -Wwrite-strings -Wpointer-arith -Wimplicit-fallthrough -Wshadow")
  set(CMAKE_C_FLAGS_RELEASE     "-O2")
  set(CMAKE_C_FLAGS_DEBUG       "-O0 -g3")
  set(CMAKE_C_FLAGS_COVERAGE    "-O0 -g3 --coverage")
  set(CMAKE_C_FLAGS_ASAN        "-Werror -fsanitize=address -fno-common -fsanitize=undefined -fno-sanitize-recover -O3")
  set(CMAKE_C_FLAGS_ASANDBG     "-Werror -fsanitize=address -fno-common -fsanitize=undefined -fno-sanitize-recover -O1 -g3 -fno-omit-frame-pointer
 -fno-optimize-sibling-calls ")
  set(CMAKE_C_FLAGS_MEMSAN      "-Werror -fsanitize=memory -O3")
  set(CMAKE_C_FLAGS_MEMSANDBG   "-Werror -fsanitize=memory -O1 -g3 -fno-omit-frame-pointer -fno-optimize-sibling-calls -fsanitize-memory-track-origins=2")
  set(CMAKE_C_FLAGS_CHECK       "-Werror -Os")
endif(CMAKE_COMPILER_IS_CLANG)

if(MSVC)
  # Strictest warnings, and treat as errors
  set(CMAKE_C_FLAGS "${CMAKE_C_FLAGS} /W3")
  set(CMAKE_C_FLAGS "${CMAKE_C_FLAGS} /WX")
endif(MSVC)

if(CMAKE_BUILD_TYPE STREQUAL "Coverage")
  if(CMAKE_COMPILER_IS_GNUCC OR CMAKE_COMPILER_IS_CLANG)
     set(CMAKE_SHARED_LINKER_FLAGS "--coverage")
  endif(CMAKE_COMPILER_IS_GNUCC OR CMAKE_COMPILER_IS_CLANG)
endif(CMAKE_BUILD_TYPE STREQUAL "Coverage")

if(LIB_INSTALL_DIR)
else()
  set(LIB_INSTALL_DIR lib)
endif()

include_directories(include/)

if(ENABLE_ZLIB_SUPPORT)
  find_package(ZLIB)

  if(ZLIB_FOUND)
     include_directories(${ZLIB_INCLUDE_DIR})
  endif(ZLIB_FOUND)
endif(ENABLE_ZLIB_SUPPORT)

add_subdirectory(library)
add_subdirectory(include)

if(ENABLE_PROGRAMS)
```

```
    add_subdirectory(programs)
endif()

ADD_CUSTOM_TARGET(apidoc
  COMMAND doxygen doxygen/mbedtls.doxyfile
  WORKING_DIRECTORY ${CMAKE_CURRENT_SOURCE_DIR})

if(ENABLE_TESTING)
  enable_testing()

  add_subdirectory(tests)

  # additional convenience targets for Unix only
  if(UNIX)

    ADD_CUSTOM_TARGET(covtest
      COMMAND make test
      COMMAND programs/test/selftest
      COMMAND tests/compat.sh
      COMMAND tests/ssl-opt.sh
    )

    ADD_CUSTOM_TARGET(lcov
      COMMAND rm -rf Coverage
      COMMAND lcov --capture --initial --directory library/CMakeFiles/mbedtls.dir -o files.info
      COMMAND lcov --capture --directory library/CMakeFiles/mbedtls.dir -o tests.info
      COMMAND lcov --add-tracefile files.info --add-tracefile tests.info -o all.info
      COMMAND lcov --remove all.info -o final.info '*.h'

    COMMAND gendesc tests/Descriptions.txt -o descriptions
      COMMAND genhtml --title "mbed TLS" --description-file descriptions --keep-descriptions --legend --no-
branch-coverage -o Coverage final.info
      COMMAND rm -f files.info tests.info all.info final.info descriptions
    )

    ADD_CUSTOM_TARGET(memcheck
      COMMAND sed -i.bak s+/usr/bin/valgrind+`which valgrind`+ DartConfiguration.tcl
      COMMAND ctest -O memcheck.log -D ExperimentalMemCheck
      COMMAND tail -n1 memcheck.log | grep 'Memory checking results:' > /dev/null
      COMMAND rm -f memcheck.log
      COMMAND mv DartConfiguration.tcl.bak DartConfiguration.tcl
    )
  endif(UNIX)
endif()
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 12 (0xc)
```

```
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=NL, O=PolarSSL, CN=PolarSSL Test CA
    Validity
      Not Before: Feb  7 16:06:36 2012 GMT
      Not After : Feb  7 16:06:36 2022 GMT
    Subject: C=NL, O=PolarSSL, CN=*.example.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
        Modulus:
          00:b9:3c:4a:c5:c8:a3:8e:90:17:a4:9e:52:aa:71:
          75:26:61:80:e7:c7:b5:6d:8c:ff:aa:b6:41:26:b7:
          be:11:ad:5c:73:16:0c:64:11:48:04:ff:d6:e1:3b:
          05:db:89:bb:b3:97:09:d5:1c:14:dd:68:87:39:b0:
          3d:71:cb:e2:76:d0:1a:d8:18:2d:80:1b:54:f6:e5:
          44:9a:f1:cb:af:61:2e:df:49:0d:9d:09:b7:ed:b1:
          fd:3c:fd:3c:fa:24:cf:5d:bf:7c:e4:53:e7:25:b5:
          ea:44:22:e9:26:d3:ea:20:94:9e:e6:61:67:ba:2e:
           07:67:0b:03:2f:a2:09:ed:f0:33:8f:0b:ce:10:ef:
          67:a4:c6:08:da:c1:ed:c2:3f:d7:4a:dd:15:3d:f9:
          5e:1c:81:60:46:3e:b5:b3:3d:2f:a6:de:47:1c:bc:
          92:ae:eb:df:27:6b:16:56:b7:dc:ec:d1:55:57:a5:
          6e:ec:75:25:f5:b7:7b:df:ab:d2:3a:5a:91:98:7d:
          97:17:0b:13:0a:a7:6b:4a:8b:c1:47:30:fb:3a:f8:
          41:04:d5:c1:df:b8:1d:bf:7b:01:a5:65:a2:e0:1e:
          36:b7:a6:5c:cc:30:5a:f8:cd:6f:cd:f1:19:62:25:
          ca:01:e3:35:7f:fa:20:f5:dc:fd:69:b2:6a:00:7d:
          17:f7
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints:
        CA:FALSE
      X509v3 Subject Key Identifier:
        7D:E4:9C:6B:E6:F9:71:7D:46:D2:12:3D:AD:6B:1D:FD:C2:AA:78:4C
      X509v3 Authority Key Identifier:
        keyid:B4:5A:E4:A5:B3:DE:D2:52:F6:B9:D5:A6:95:0F:EB:3E:BC:C7:FD:FF

  Signature Algorithm: sha1WithRSAEncryption
    91:b3:84:5c:5d:60:f2:a5:0a:4a:dc:d6:c6:75:da:34:52:72:
    6c:0e:60:4f:ef:0e:55:f3:4b:bf:d0:40:e7:91:2c:a7:94:8f:
    3d:db:0a:ec:b2:f5:83:a7:a1:33:61:96:37:57:14:80:5b:e7:
    bc:e1:d3:2c:36:32:6f:ef:7a:00:99:33:15:fc:38:20:df:74:
    7d:3d:0f:81:d0:b4:fd:b6:46:f1:c5:b8:bc:de:74:a2:41:a7:
    c8:51:da:20:12:82:3e:0c:8c:48:da:19:b6:52:e9:4f:67:c1:
    28:9e:20:b6:ce:be:89:bd:64:d7:05:3e:87:af:ba:2b:5d:aa:
    fe:62:66:fb:a6:75:ad:89:a1:18:e8:78:54:ea:df:0a:85:e9:
    32:32:a8:1a:cd:35:81:f8:a8:da:d1:16:8a:63:e7:67:da:6e:
    e1:3b:1c:31:20:99:ee:e2:b2:fb:82:c5:21:e2:63:4c:61:15:
```

4d:53:ad:dd:15:7f:0b:b6:33:43:ad:27:8a:b1:af:93:17:72:
c4:be:31:26:93:3c:7d:fc:d5:3d:cf:0b:be:c5:7b:e9:b4:f8:
f3:30:f2:f5:a2:27:eb:9a:71:fc:7f:79:5e:88:c5:a6:2d:33:
57:ba:38:06:e6:ad:0b:96:97:9d:cc:94:7b:83:09:17:a6:ee:
ce:bb:0f:36
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIBDDANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTIwMjA3MTYwNjM2WhcNMjIwMjA3MTYwNjM2WjA4MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxFjAUBgNVBAMUDSouZXhhbXBsZS5jb20wggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQC5PErFyKOOkBeknlKqcXUmYYDnx7VtjP+q
tkEmt74RrVxzFgxkEUgE/9bhOwXbibuzlwnVHBTdaIc5sD1xy+J20BrYGC2AG1T2
5USa8cuvYS7fSQ2dCbftsf08/Tz6JM9dv3zkU+cltepEIukm0+oglJ7mYWe6Lgdn
CwMvognt8DOPC84Q72ekxgjawe3CP9dK3RU9+V4cgWBGPrWzPS+m3kccvJKu698n
axZWt9zs0VVXpW7sdSX1t3vfq9I6WpGYfZcXCxMKp2tKi8FHMPs6+EEE1cHfuB2/
ewGlZaLgHja3plzMMFr4zW/N8RliJcoB4zV/+iD13P1psmoAfRf3AgMBAAGjTTBL
MAkGA1UdEwQCMAAwHQYDVR0OBBYEFH3knGvm+XF9RtISPa1rHf3CqnhMMB8GA1Ud
IwQYMBaAFLRa5KWz3tJS9rnVppUP6z68x/3/MA0GCSqGSIb3DQEBBQUAA4IBAQCR
s4RcXWDypQpK3NbGddo0UnJsDmBP7w5V80u/0EDnkSynlI892wrssvWDp6EzYZY3
VxSAW+e84dMsNjJv73oAmTMV/Dgg33R9PQ+B0LT9tkbxxbi83nSiQafIUdogEoI+
DIxI2hm2UulPZ8EoniC2zr6JvWTXBT6Hr7orXar+Ymb7pnWtiaEY6HhU6t8Kheky
MqgazTWB+Kja0RaKY+dn2m7hOxwxIJnu4rL7gsUh4mNMYRVNU63dFX8LtjNDrSeK
sa+TF3LEvjEmkzx9/NU9zwu+xXvptPjzMPL1oifrmnH8f3leiMWmLTNXujgG5q0L
lpedzJR7gwkXpu7Ouw82
-----END
CERTIFICATE-----
Standard PEM write
mbedtls_pem_write_buffer:"-----START TEST-----\n":"-----END TEST-----
\n":"000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E0F":"-----START TEST-----
\nAAECAwQFBgcICQoLDA0ODwABAgMEBQYHCAkKCwwNDg8=\n-----END TEST-----\n"

PEM write (zero data)
mbedtls_pem_write_buffer:"-----START TEST-----\n":"-----END TEST-----\n":"":"-----START TEST-----\n-----
END TEST-----\n"

PEM write (one byte)
mbedtls_pem_write_buffer:"-----START TEST-----\n":"-----END TEST-----\n":"00":"-----START TEST-----
\nAA==\n-----END TEST-----\n"

PEM write (more than line size)
mbedtls_pem_write_buffer:"-----START TEST-----\n":"-----END TEST-----
\n":"000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E0F000102030405060708090
A0B0C0D0E0F000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E0F":"-----START
TEST-----
\nAAECAwQFBgcICQoLDA0ODwABAgMEBQYHCAkKCwwNDg8AAQIDBAUGBwgJCgsMDQ4P\nAAECA
wQFBgcICQoLDA0ODwABAgMEBQYHCAkKCwwNDg8=\n-----END TEST-----\n"

PEM write (exactly two lines)

mbedtls_pem_write_buffer:"-----START
TEST-----\n":"-----END TEST-----
\n":"000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E0F000102030405060708090
A0B0C0D0E0F000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E0F000102030405
060708090A0B0C0D0E0F":"-----START TEST-----
\nAAECAwQFBgcICQoLDA0ODwABAgMEBQYHCAkKCwwNDg8AAQIDBAUGBwgJCgsMDQ4P\nAAECA
wQFBgcICQoLDA0ODwABAgMEBQYHCAkKCwwNDg8AAQIDBAUGBwgJCgsMDQ4P\n-----END TEST-----
\n"

PEM write (exactly two lines + 1)
mbedtls_pem_write_buffer:"-----START TEST-----\n":"-----END TEST-----
\n":"000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E0F000102030405060708090
A0B0C0D0E0F000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E0F000102030405
060708090A0B0C0D0E0F00":"-----START TEST-----
\nAAECAwQFBgcICQoLDA0ODwABAgMEBQYHCAkKCwwNDg8AAQIDBAUGBwgJCgsMDQ4P\nAAECA
wQFBgcICQoLDA0ODwABAgMEBQYHCAkKCwwNDg8AAQIDBAUGBwgJCgsMDQ4P\nAA==\n-----END
TEST-----\n"

PEM read (DES-EDE3-CBC + invalid iv)
mbedtls_pem_read_buffer:"^":"$":"^\nProc-Type\:
4,ENCRYPTED\nDEK-Info\: DES-EDE3-CBC,00$":MBEDTLS_ERR_PEM_INVALID_ENC_IV

PEM read (DES-CBC + invalid iv)
mbedtls_pem_read_buffer:"^":"$":"^\nProc-Type\: 4,ENCRYPTED\nDEK-Info\: DES-
CBC,00$":MBEDTLS_ERR_PEM_INVALID_ENC_IV

PEM read (unknown encryption algorithm)
mbedtls_pem_read_buffer:"^":"$":"^\nProc-Type\: 4,ENCRYPTED\nDEK-Info\: AES-
,00$":MBEDTLS_ERR_PEM_UNKNOWN_ENC_ALG
00 0
*H=0>10 UNL10U
PolarSSL10UPolarssl Test EC CA0
130924155204Z
230922155204Z0410 UNL10U
PolarSSL10U localhost0Y0*H=*H=B7Vv Zr>Y- n|th"YbN#/4]]kw
U*00 U00UPaecF0nU#g0em $I?+x~$6|B@0>10 UNL10U
PolarSSL10UPolarssl Test EC CA C~bC0
*H=h0e1,\d
Na1ssT]/!)5>90!6]'%;5%Y^|f{Os!R*
-----BEGIN CERTIFICATE-----
MIIDijCCAnKgAwIBAgIBKjANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTQwNDA5MDg0NDIzWhcNMjQwNDA2MDg0NDIzWjA0MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxEjAQBgNVBAMTCWxvY2FsaG9zdDCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBAMFNo93nzR3RBNdJcriZrA545Do8Ss86ExbQWuTN
owCIp+4ea5anUrSQ7y1yej4kmvy2NKwk9XfgJmSMnLAofaHa6ozmyRyWvP7BBFKz
NtSj+uGxdtiQwWG0ZlI2oiZTqqt0Xgd9GYLbKtgfoNkNHC1JZvdbJXNG6AuKT2kM
tQCQ4dqCEGZ9rlQri2V5kaHiYcPNQEkI7mgM8YuG0ka/0LiqEQMef1aoGh5EGA8P

hYvai0Re4hjGYi/HZo36Xdh98yeJKQHFkA4/J/EwyEoO79bex8cna8cFPXrEAjya
HT4P6DSYW8tzS1KW2BGiLICIaTla0w+w3lkvEcf36hIBMJcCAwEAAaOBnzCBnDAJ
BgNVHRMEAjAAMB0GA1UdDgQWBBSlBehkuNzfYA9QEk1gqGSvTYtDkzBjBgNVHSME
XDBagBS0WuSls97SUva51aaVD+s+vMf9/6E/pD0wOzELMAkGA1UEBhMCTkwxETAP
BgNVBAoTCFBvbGFyU1NMMRkwFwYDVQQDExBQb2xhclNTTCBUZXN0IENBggEAMAsG
A1UdDwQEAwIDCDANBgkqhkiG9w0BAQUFAAOCAQEAriPloIWfu7U8d1hls97C7OBI
OiE2xFh2UmuN/9hTK2CyW6MtBf8aG3l4jQDrsutHO0gUyoR67ug4yj+s+0S/zETZ
q6mPo7cBbVwjhGciQRiYgufFpdnbXR05HDgOVPK7qqjL6UOZnbu5caIEvIJgdwXn
n8WB9x/Ii4/2S9ysmRdRhDBYekzgH3Ac2UnHJTMh1XaSL817MW6B9BDKHt4xa7pW
cplDzrFKYbmxSSxzALE4Dr+zRvmDx4bcYpBkRRfOhnnR1caQBgaZzPcX/Vu+vw8e
qs2nyBW5RBu8MBCBU1DpqOSo6jl0QTpuq3NzQZIouG9fyckqDJS5ibrxQTutPw==
-----END
CERTIFICATE-----
-----BEGIN X509 CRL-----
MIIBqzCBlDANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDERMA8GA1UEChMI
UG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EXDTExMDIyMDEwMjI1
OVoXDTE5MTEyNTEwMjI1OVowKDASAgEBFw0xMTAyMTIxNDQ0MDdaMBICAQMXDTEx
MDIxMjE0NDQwN1owDQYJKoZIhvcNAQEFBQADggEBAJYuWdKPdblMVWCnxpMnchuL
dqWzK2BA0RelCaGjpxuwX3NmLDm+5hKja/DJxaRqTOf4RSC3kcX8CdIldsLO96dz
//wAQdFPDhy6AFT5vKTO8ItPHDb7qFOqFqpeJi5XN1yoZGTB1ei0mgD3xBaKbp6U
yCOZJSIFomt7piT4GcgWVHLUmpyHDDeodNhYPrN0jf2mr+ECd9fQJYdz1qm0Xx+Q
NbKXDiPRmPX0qVleCZSeSp1JAmU4GoCO+96qQUpjgll+6xWya3UNj61f9sh0Zzr7
5ug2LZo5uBM/LpNR1K3TLxNCcg7uUPTn9r143d7ivJhPl3tEJn4PXjv6mlLoOgU=
-----END X509 CRL-----
-----BEGIN X509 CRL-----
MIIBcTCB9wIBATAKBggqhkjOPQQDAjA+MQswCQYDVQQGEwJOTDERMA8GA1UEChMI
UG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EXDTEzMDkyNDE2
MzEwOFoXDTIzMDkyMjE2MzEwOFowFDASAgEKFw0xMzA5MjQxNjI4MzhaoHIwcDBu
BgNVHSMEZzBlgBSdbSAkSQE/K8t4tRm8fiTJ2/s2fKFCpEAwPjELMAkGA1UEBhMC
TkwxETAPBgNVBAoTCFBvbGFyU1NMMRwwGgYDVQQDExNQb2xhcnNzbCBUZXN0IEVD
IENBggkAwUPifmJDzOgwCgYIKoZIzj0EAwIDaQAwZgIxAKuQ684s7gyhtxKJr6Ln
S2BQ02f1jjPHrZVdXaZvm3C5tGi2cKkoK1aMiyC3LsRCuAIxAIMhj0TmcuIZr5fX
g5RByD7zUnZBpoEAdgxFy4JPJ2IViWOPekSGh8b/JY1VNS6Zbw==
-----END
X509 CRL-----
HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 0, 0) #0
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"a0c9ab58f1e2e5a4de3ebd4ff73e9c5b64efd8ca028cf81148a584fe69ab5aee
42aa4d42176099d45e1397dc404d86a37bf55954756951e4":"":"":"":"9a00a2d00ed59bfe31ecb1399b608148d1969d
250d3c1e94101098129325cab8fccc2d54731970c0107aa4892519955e4bc6001d7f4e6a2bf8a301ab46055c09a67188
f1a740eef3e15c029b44af0344"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 0, 0) #1
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"07bddab06cf3d7f094cc2302abd700a9d67421aeb711f4bbe66f59e28a46794
213bf3d0c3a2cbbb09205b90e0ef212c7679b37526a806789":"":"":"":"f76fd2a49d9574c3f90864f35f32253b83098ee
04a4c8dba464a8035f665ca165c8a038be5e1b100d56752adcf59bea167e15b1d01c419948d2d0a85be66d19bb40e5e0
a66cfd76ba7547eba6276ea49"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 0, 0) #2
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"6d283e7705a2aa4b1abfc1ff8559c9e7962df9229000b8e432ac40bad347973
45f1ed6d7a0fdea8ec01e7a20dc436aa1d62153813d59d44a":"":"":"":"60ddce57be4563b87bb59e848496f42fcef9ed7
9799040e0eee68fd89b330109cd3b3f761348fc7036c0cf5d69aefecf91e89a7ae0429590569a88922aeff249ea783f00f7
95aadca729f96996eef76d"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-1, 0, 0) #3
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"108a1fa539fc471e0a26a8d39633c88d1e84c26a62894e7dec15fcbeda9dcd1
e40619dc03c7d3dd2db39bc8f4964949b1737b9cd69a8ff97":"":"":"":"b0fbe3f6b6667b88e2a48f3679f21ad83f28107
675d43d2a5186dd6a0256afc6acaf995b3f07691325543b37ddd5bfb4934f46ff9783597b69c727c9cae1c6b83601a392
27c53c99181ec18d5be60d5b"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 0, 0) #4
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"1db6fe209a51124f9eba3ae7a5690a31c9383b0d62abe0237fa6ce2b34b320b
68d24927d9245a10f7216ded701c39f4d10dd6eb4ae912b78":"":"":"":"10e9661bbe14a0c768f09840979233865296fa
801ee8ba97106043c067d3b01a5d3a866eb9b21f730c3ec1f11f022820a2a2db4cd07061acb85b0987e33892064b5662
6c962d1febe1eb97af6b99ac22"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1,
0, 0) #5
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"dac7cb5d659646246a2c3cd6cbb8b7bb9ede30c88355725c16576ca7567f52
b51ea3f7e5d456b0e8b7a33faf21150e5b39999ee53fd05b2f":"":"":"":"7117fe0c0a9afa75c078b1641ba637ed2a4501e
70bf38465914ea185da5a62048910040e70f279ca9f2fd5e478ffd76484f52afa62a29ca9d649f252f27a8eeca1ec95d789
8f705421c92b60493e5c77"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 0, 0) #6
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"a422e11d41ed91e458b1dff7844e7a06eb807b042fec7c42da9a7d64aea6ec8
43cbb5dacf8517c3f7214d02d432fc64766f6bd40f54290c5":"":"":"":"e6e1b59d47aa47ebd862fa2336d50a920f77aff6
d42942a293947c24b044756c9777231aa0ce8a67d2916136cf4477dde78b6fa789b4a570460538a3da199c2c64155692
bc1aef3fa94ce8ba4a43bcaf"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 0, 0) #7
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"8020ccd23e6733f7638a6d68b4954b701dd2e3b33176d5d1a14b6cd8aead4e
152e0726dd16b4d76dd9cae60e69023d0fd82b0b69b7cbaf75":"":"":"":"c2b22410ddba0466b6635ab98f7690572d71
59d66b4f037fa75869276950ea4ab4a92e3011d7c3d50f921a3988906486590706c8e0eeeb487ac85ca924d8b3a4445e
2af49365c10c6e99eb17d93286c3"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-1, 0, 0) #8
depends_on:MBEDTLS_SHA1_C

hmac_drbg_pr:MBEDTLS_MD_SHA1:"d66ef5d12c778d8b78134704e345b08c6839471eb903bd0480169d4069d73a669a17dff2e1d6fc23f0688fdf7867f72a024ae445969458fb":"":"":"":"91ef2bacbffacbedc11da58d275448692ae26bb9920c0b14d86a42a65a9a79422ed77c3a8f941b428552caf6d15e057c2dd8b5cdee670ee151f674b4a82ff9754cb067c1a1a27302bef2d395379d6009"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 0, 0) #9
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"cb4ca0d6e07b341ea0d105e5128bcd6b6fc317bec49394a83c485ce4f8205361374484ac0173ef3f08fd65d0a11af2b3f90ee8bd3fcdc08b":"":"":"":"1727a7f580a267492646fc2c18e3539a131b52fa3d82ac8cb36227ebb94a396b139c0a709301b4f00b49ec63d7f48125e469443b57b16bdab66bdaf0684da425e63a596182de4674416ade17f0cef49d"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 0, 0) #10
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"7cec0120261bbeddd34eb776464c9b80667da732cc82c365a492b4def218ba2cad59f7b4bc1afaef00861c9b62b581444f79b8977e9fbf8f":"":"":"":"3ad128a75af8144cdf5cace68166dabca9db5d5cac6eeaa0c3d608d99d5da4a2ca90fc080d832e5f97060ab2247dc5dc20bc10be47e6ab03efeb662fc9d52c89d8db340cc4903be59dfd086f6d018468"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-1, 0, 0) #11
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"29dc07553bb77cad6f321bcdd5c5c758b6a77588ee43d0afb15c0d981e368cb2482663aea93ded95d82a1a2a22cdbdf8de93695862cd9429":"":"":"":"5e1d53d8db89511fa996ccf513baacee2612da201c21d51e2927dcb99caf3132f6d2ccc3376dbf95520018515b0784e98b4226671cb3f1c7915757d2e59f1c4e843ea9c98004108118b4eb53bef2baaf"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 0, 0) #12
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"748777316160fc175eafff578481402ccd5a38508e4ac0603f86281576c970d3316ee58a36f809a8df9ef241861c04093a284d116384d204":"":"":"":"05f179c71691c0c2c64eda58b63a27772210f0c2c6973708a5f84e6b49f547169a839f2e97ce18ac94696337a9d1c1d450bf27b7fdaf1761ee8da9b55d59031a8516eeaebb1bd48a1e3bd070c5fb4eda"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-1, 0, 0) #13
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"11e2e3934d23239aa6bf1abb07aadaf8df05892d126cd4be13f2965bdcfcc8396dcb16d8742eed1b276b562702915fbb59c01cafb7044022":"":"":"":"6ec1caa762b5b87ce92ef7d254536f94d41ed5a98696da5c14fa2d29aa95182927b3e2a5ee9e2012c911ecc5e244af1a8200de37cbff2b26d0c2271659bce074d5b3c06743f08d6495286068a1e5435e"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 0, 0) #14
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"ec11e1929e7430b914b385285801e27df4aa6783fa1e3405ae706e740dda50209b20acf90dfa8cecb4d4b4bc7cba4daa285ff88ce9e8d451":"":"":"":"74acba48f0216087f18042ff14101707c27d281e5ddbc19c722bec3f77bf17ca31239382f4fc1d4dd0f44c296bc2f10f74864951f7da19a23e3e598ac43fb8bbdd1fca8047b98689ef1c05bc81102bb5"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 0, 128) #0
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"d92b39ff610db66427613c111c002b75329734372847a88f53c1d289b30d3584d34efb884ce6d1d7174a3c20508ca0171ed9610622d454fd":"":"9980d97c65cc8b3c61b390e48abc6523":"76213356e359e94984cfa7db15220518":"e0b298f7cd1112527a506201e38f7e60d762f591603db72aca3a2cd1b9d115c3ddbc7dcb7643f2f40f53e96e6ca1590ca27abb77a6234754ff1edef86f75fd5f298872ad1544fb88a62936e238f22aef"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-1, 0, 128) #1
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"3c56bd6733e9cf9d765f3d5906c60807bd1c9c11f4a1293bb4abaefe6a65c978d9c75a704239e500319d9b4b8f9f121caef7fe3c49f9ab37":"":"365f1612ecb78ad7b1140dc66082ab30":"0e5d2013782191581e4a76e0a2b5bec4":"0e509b7b436d085c1080c3d9e6ee3cc563944bba0fad352d13182c87c8c3a0f0ba71e86676729da0d2f4acc2b57e430b8791c4f30d232a0fe48bf91d5824242fb8e36333837173d702e6738291b57efd"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 0, 128) #2
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"91a44f3e412d031bd47ec8907e32f0434a20d784db3f6ffd78b013ca0b00553698a113d75d8ebbe856554c71aa4b0d48af74bbebc97afab4":"":"9f4b3b3f1e2d849753d2cedc8d8c5d17":"64a1f4d2b10cf97a268cae7034ca4d8c":"232ade326de23ec970f66e6a540f306d962769d1b24b0675109ca7514dbc52003d154687f525f4a2220501d6dc92551df9111c8dd398356c560ce44f1959301dedbb197c0161fcad0299a9eef3e799e2"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-1, 0, 128) #3
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"fbaa5e65ce5580d774739340e025eac46550b5d3865829eaef9b59ea37d094692b9fd15ca25468fcf7e38f7dcecd5fd85c686057e1ab9bab":"":"f0e722190994c66f64ff725e8a9b3be0":"548ed3bbccc8f9f79c70b2e85ee0e626":"2c07d2994fbf0bbefbbaf60e0dbc712f12f8ddc3aa6d94ea9e9d3083209ec35c4cf3e62bceb9ab042e60050520e0469961dbdaee0787fda6f1c49755855752753b1e87031a6821c04cda887cdedecc55"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 0, 128) #4
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"13747421a19855709f3c468a5b1f77c19eb589a0b18c06da3aae0078b85ee10c79d1925f5ab2045eac1f2ffdd850e7602cda7debeb042bea":"":"3c95ff221ccf82f4041fcf4e8a56de29":"3471a7ab4234fc6e8678d3613ee10835":"c346efd443cec6f21eca26eb5289e0bec5eb3f7c3785842e7690d5d35eddc87d79041aa0a9d5e4ee9ec69a4b67b26ccb70eecb59df582316b8f1b945a25c64b861a6decb59adc1447cea219947f6aa72"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-1, 0, 128) #5
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"4f72d884628c90261fdfa9b87bdbbce93daaf175d0290ae7f725e8a9f9b8c98807b57a591d4e8b2a5b692a6e310c4851bc4a6d986eba9cef":"":"8b3a7401800ee1bf5fdc76243b313244":"cc199f4f43036b0af63fe3f8ef4ab3d2":"6950a89759b52b6c8416600f9e0d56d19fab12b423d746af9d00a6657f3b8f3a3681c0910343569544b8b537294aa610e89b977c4db21a324317587be8b9232b38d354eb3e4032cacd561dfe42e72d23"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 0, 128) #6
depends_on:MBEDTLS_SHA1_C

hmac_drbg_pr:MBEDTLS_MD_SHA1:"59c23b4073e7c9d2871d5d882953a33b17eb2a8b0b9b068870c070deb9f13
24b8fc29fdb612c52dd300889913ab120536cf9a389485859bb":"":"a6483a9e5113a45a84f6630869291461":"b93bbb
79da7750f44e4561081ac4f29e":"6a298856c9b25b20de0159890135beddc415802307b87507d62b2ad32b1883e4ba0
36308a6669a06246d4afc43a29e183ca141f156f7b1975095bf14cceaf71cd2831fac8870d90fe0e1067434783a5e"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-1, 0, 128) #7
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"a4b620abe19aff576cddb8f6d1e83b59c26d4ba79fb8346974ca841db33e280
d59e28e110cfeafc4f033c6a45f443f528a326ed4c2de5cd9":"":"be26760cfc23c0cad1ad0978c3ec8f09":"e767cc66942
42b003d6d3795415389b8":"89d79211db69679c2269dfb2e599740ff646eb9ebd5f28a68b76665e6087d15fb888bbf89
9e3d16d711c3db63e3dbf9cd9bcaad6984be04afe5b41c2270431948ddf4486272f136f1c5bdf37cd2a70e8"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 0, 128) #8
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"994e455c4815ffd4a9ee168d1fccd3b661da827c4e81b102db0b28977c81bc
4dd58d06819e2939883983f9ebf1356b0d01e6dc02735596ca":"":"029caa66544f6ae8f6cc5bd3791f86f0":"7f14c05c5
d88acafab220aa467e3e3ca":"fde93e19f71fa97fc368f5f4454df8a39b3fce42bd4a801726b296838c3dcc6678bb38768
7e2c943edab86902e377a619950d36fe78cd7ba3c67aaecafdd9f7faa2076d71fa79646933387bd6bee147a"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-1, 0, 128) #9
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"2713eb063d3876dd6c3a5903a1ef5774a180c4123eeeea8a4aa472cf07c278a
c367a9a490c7ddef058d6bf34ec9db314abb119a1a017a17e":"":"4452362eed6b9c30a01f784a9a06dc5d":"e59780f29
1461d2665924f3af8bcb6e0":"743f529bee048d0be6f10da0101c63c746fbeed37c6cd0c0ae97854893a00c82b65acc9e
6e6ec04357e5e4b3159a4ef3e5e57a38da2e00f0eb3c1538a26ee1a518f71169d59b0d9e8a021f3d623b8fc5"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 0, 128) #10
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"ff2cb4930d26b0ee75bd9edfb77e09f50c80049f75ba95a5137ea862d086d65
23bdfde203bb8c2a9bb588ef2428a173453136bdedec37eb3":"":"a52775c066b6e9f7508b30ca22944296":"5e4ad554
e65a49685e8527f923cbc0cc":"4e9134db809bd07a46f40bc1a1f6d830808121eed25d17d7ce3eb81bb88ec660b7dd94
5ebe9fef8bdccda92139f4770ab8a467e0118f24680c6f6e5b9ad6ee94a086118b6cf69aceb8cd809d91429aa6"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 0, 128) #11
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"72971d13d6356e68fa61d94ae1d76a91b69d8b39499393fe9eb2889d14d91a
7488207bd8ee536d481b37237b0995a218fb56dd1740335992":"":"0e59b74d4ac5ab8bb51c7f4b99ff859e":"232dec6
0628a43216b75839ac820fe4d":"1f1adb85b8d7d1e022d5a6594ce074242683993ee4d3c5166a2aaf40c239830587b11
12af2a4313e363ea4a980b06f20c5ee3207de026aaea9197c95d0e771f4f16a2cab41c0684c15e6462cb7a5a71a"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-1, 0, 128) #12
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"975c10933f7351262a4296aa6175471fa34e7c9b3437b5c7013e22d2a9002e
9e42d27202e0518b53da23016d1f5b7b63c46c1391886934d5":"":"b7063d6ba3740d5c258303d5393f8f3b":"916178
0ba6bef05da7290a77416767ba":"b68b4ebb6856af7337745e0a50caa1d34abe27594d56d846794c15bc03973d67d54

8bbd2680dc749c5171372e27af16900d6bf729a84e6d7626563ef0b4c90c275d9112567b8ca6e0093b34a0966f27d"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 0, 128) #13
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"e1dfa7999006aee12a2349ae1d580f5ca2a437dc0bc294f449f2670afc55e8fa8152c787a014880f670c585cfca574ea2d13f28e6a0ea677":"":"d77a830f650a3331a72f0a4b1471dab6":"37aef81e729ed0b91bf054ce98df4a76":"c009a692d7e566b58cc54a45f7d6987a48d96c3664f6034ae3ac0dae9ed5c220c46ef0c638c75353ac790124d88ca54fe43797f1a70422604507a2ab458fed576ccf6d25cf521da8d0c3b7bfa16ee6f6"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-1, 0, 128) #14
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"310d8d08687545e48493db179e6e92a176cba53ff17cd783ba5d38da5f2e51468b0a9489c88b8db0be4a2c87c875be0e1be01aadf2efeef6":"":"a1824b07e0d2ada0fadec29beb53a9f7":"ccdb3f7d7f6a4d169f5f2e24ec481fcb":"bfcc8f2ece23d22545ec2176aabd083855923ca9a673b54b66a3e2562212aad3cc74c4c8976de259cc95a2f09a85b7acd1f18c343eff0368a80e73a547efdcd954816b38df1c19556d714897e317d69f"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 128, 0) #0
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"db8128c27eaf3a39d5019785aa35b20c3977437fd75e8032ed340ddbe1b29eb9bedb3048a3fdd06aa957c5cff00eb87549c307400d4059d0":"4f8060506daf40819c7c58630151edc7":"":"":"4ac933b7de803c266461493a19dbb00e9db25ee768165781fc9a70c67c4e8a92db36471e3cb1714fbb65e17d74770061b0abae52be34a604d87e56a4ae1e90c6533cc764aa7419b5439e3efa193934bb"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-1, 128, 0) #1
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"87c80a5e334e02a36f59324befb4fae19e5b73aef691d45e8973f58a487b457d73c4312ff890b053472d95de538f1512f6432233b7d9c058":"6cc5553434148499d65f8e4ab7334938":"":"":"5ccdcb3d022eb4d72c211594c916dd2d883d2ecc190f6e78ed76f438562059e6f8800ce6d11b3b8603243f4a56f38d41672935ace8d6fab825cb6978a2d0827aa65c70523c48f7b9a8f6fe43cc2ba927"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 128, 0) #2
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"83c113dabd43229d4a7333147c7d84f48fc29ea3d813c0f1d45c5184906a02ea4c6f11b149db7f98812904be3ee96de25ac9a78ccdfddeb3":"77dc45d37d6d401e45c982f2c4960fd6":"":"":"e4f08087eaae11fca94bd7df816980e6608e208032f944f1efc50ac8d47834b9f10c00958837633e61f3ed2351c6885446b72d2634bf6b69f9d7b7a36f3fb8e98294f1e9d92a4a725462e60325dc41ca"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-1, 128, 0) #3
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"aec809c1b7eef916569cca247cd9e7b072df669458c8af4d29fecba0c46130ba920fc8bf7d29cfaeda476607f3325566ef52fb69a3defc54":"824b11ac7e13f654ff4238e0f28a2f60":"":"":"514f1adaeb99dd2833f714a53804aca43a99fce45caf5db166b15acb0460f5e7e23c696fdaa8ecd138a937367483dc7bb7a6af51a611aa7b0671559aed14109133738e06bf2190bb85abef3a674e488a"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 128, 0) #4

depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"b2f5cacdf871e742c262c7671b59a74c6a41242b2225f252cba7db3bf77d6619af46532eb9c01b72cde2978ec39e4fe5247ac5f0fea559d8":"2cbfb9bc6c318219df86e08ab11419e2":"":"":"67d393c84d05983f5acfb8883ed44e24406f216efa3d6650807fabd3028fb1f762d6c67ffb0aabe8143fd3ddfda8ca2c7ef13546dcffc4dcf95b610a28f7cc2a25ac4e7ec0944d655c56c110fa931ff7"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 128, 0) #5
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"54ef54d0425f8cebd127fed0f395884613dc19463664d19d02af6baf06de126b55fbb3d7f114728bb4650839f1335f8c2c3be18ea3beea75":"f0cef260a2f74a425d062bb25c68c539":"":"":"dd8b96a5f3fbd0f5f69477c5b7e71099b2113888fcfa6acce713a13f040b0b5fd55100a3d0d3a344706a31e796d6999f63cc6357f5ba386f38d46bca9c42a25c4a39afdc7db8d843a032ef35bf4b15ef"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-1, 128, 0) #6
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"4a1781c483eae07e0a9ddd91b908fb00a21a4f5e1c6e9da58f380f407dbcc982cd0761e5f0fd6d339a646bdc6132addb7ac0cdefb1b91f7d":"c4b7084d73d399c128e0a119217c793f":"":"":"e465cbc1502709493de1d3347a07f855b2dd6435a4ebaaf00e7756c1439219546e5fc67093f0eac1055d221fde51297cdc9ff41121d582514c75e9906870f99d58806f1873f0183277510cf1f067a840"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 128, 0) #7
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"36974a7c276e18ed2704eedef6b627f8e57e755d554b80efd0f065c236f78964cfd3b661405b98640631fda19fefa8b5b003e8b752ef060b":"626a8bc0d1fab08c8c6afcdc3dc6ac33":"":"":"6b9ae340e5e75e1dcf6f181589a1fdba3951417c30467be4b41e9ff4ce03073ef1ba0a19d160abc8e5e23ed433bcc421ff1f428780454defb66511fc94794f3ec1c48c014d783bb173db102275b64b1f"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-1, 128, 0) #8
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"05f934d668e9630a131ac51e2560e45a78ceb8ef6fad7190045cd995039bfb3db624f4687302445fad08829815e7407fc962afe2779589f5":"8536223ee0184eb43e84a07cf71d445d":"":"":"97142414252556f5d5efafd39852d7a84e70316a0aff7985ed6761798eec57621271977bb950187a290dd4dd514b7a801c98103d4fd4012afdfe0f264bfe3f6e584768503831ea0211fe0415a0f59324"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 128, 0) #9
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"e2ee5b3970ac4cb83061e5692b349df8643b6100aac55ab296fcaf7a2ef7e3a1aa54c3fb1963dfd93781ca34a95d6fc3250762bd1d31b0b4":"71a4316ea88341dcf3c9280a5cb54b7f":"":"":"bf767ed7e5f11abf1a6aa5c453fa124401297e32f23270c8d78423a98f5e6783f3e8e835aa734b36c2f11be30acf0b598c7a23ac40ce894689a24fd8de3e0812e9a5cc1791091c981bfa9ec2168daf90"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-1, 128, 0) #10
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"32bd60df5e2b435c922a9e434f5f99be9c5437ff159c7e5e67b81b82f7b5ecdf6e60ec4789820d37a1071d7b91cf1e3d14f10ef7f34922cd":"c759e4ab6c8fe8a11a1f8472b06eee0f":"":"":"329cc8110

5343bd74f24c0a59b972892e789ea20e46ead1a74e7af036a836d46c70461c52df5038282e53e2db44143590d6015809db56754b778a2a7278d5050eeec9332fd732c9c714a676563c8c3ef"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 128, 0) #11
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"ac524ec09761670b96563803218a7d3589bd8e682b2a5cef64d96b968ec98839a97a4704a7a5b2b859f3ed6c370031f1027def8fa0672a26":"1531a17d3d89c1d0775f3a630ba730b8":"":"":"47e3bfaa2cbe4b085603991aa739363a639b064dd9120e0149cb5ba2ba0539c4147897a34d98538935fe25ab36cf50f6a1c3aa2892e2c06591e4c2bccfa990f6317732d5581944c8d2ef96d0329ac574"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 128, 0) #12
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"2c9a43ef1496352ea62ced1c345de4090a9cea6898b8a53abb2f01a435ec6d2050a692b44fa152bfc42ce4ea30ef761297c1ef132839d411":"00bfb2ff2600fe1dc6a2d85642e9eced":"":"":"193d08bfb22121deb22e8079895703e2a518b79bfc3104038c2a220f6babeb8f28f5652d5d1b3a8b468d8a4ed0cb32c69c5519ded85ddc0fea62d77ec5158b6a55caec3bbdf1f6b93e449d6f15cce26a"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-1, 128, 0) #13
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"0f15ec0c8d3c184d9b2a47bf9ffa20982685161bec91fad2c55808ccafd46ecd18081738cf835e1347e7df7e3f879f3fbb759c2051e34217":"eaef27215467d7878106ba9dae990bef":"":"":"bcf79ad50201f3498cf18288dc30c32dfbf2739490c74862d5e9c66b16195590075cfe094956e2bcba2009b64a5f8b62d144158180835a7f51b706a12884e309ab4ec198f5bd07efffd591d5cc8569e1"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 128, 0) #14
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"56a0b6194153e0d2737f49f4e5cb77ba4d8fbf9914405833f324c09f96434ceea7e756fc2f55a0b3f043b6e11fc2f671ec00f4d478b791c6":"81a85cb2b6afa99a1f609f83c3b15105":"":"":"40e87b822b1000441884a38b8776baa69fbea99962571e8a20d8af012d50c8c211860ad579869ec880320ea8057d5cb0de9496ec57d8b594ca8be5b94219eaa800af7205f8a83b66c87e0fee9aa9732f"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-1, 128, 128) #0
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"680face90d7bca21d4a0edb7799ee5d8b7be9eeddd0e3b4b7cafe231630aa95a742c4e5f5f22c6a41c0d7792898827948a589f822d1af7a6":"f58c40ae70f7a55648a931a0a9313dd7":"dc3663f062789cd15cbb20c3c18cd9d7":"fe85b0ab14c696e69c24e7b5a137120c":"68004b3a28f7f01cf9e9b5712079ef80871b08b9a91bcd2b9f094da48480b34cafd5596b0c0a48e148dabc6f77b8ffaf187028e104137a4feb1c72b0c44fe8b1afaba5bcfd8667f2f55b4606632e3cbc"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 128, 128) #1
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"b481041a75b03cdaa07784e372b376897fa9e792e1fa5e078d4c7234fb9dc3f9804b4e48a32a5db74990333c4951d02823765f90a0aa8850":"f8f0f1ed3f0bda164e596ebe123b7f75":"3120e329f1d55a8c07e7472ac77e1720":"2b9ff310e63c67b5e0aeb47ff7a102fa":"7d6b3ab84bb6c014dd44eb1266fb3954f1e8ff6c48a4d91514f685f0642497cb1936a0afc40c8ddd1545204e128fd06d4d18bba05d1294e64d57a0593b803a311b37cc2d631487ab03a00fe288e5e745"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-1, 128, 128) #2
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"aef9d310cfced29873b7e2b7be37572b76ed84b043364cca611917f9b12053f919cdf60ac9c0b364909f096204f21b58b0bbdcf38a3be7e9":"67e5aa83fa572ca27acfcd27d4f5e49b":"7ae90f7dc220bf5b387ed44c2425af29":"9d750dc13c19acf3cdba10155d3ca5a7":"892776bfb009fe0b1793c0ebb2ba549cbcc4a29d0374070683990c3f2c622ee08977fe9361c59838f068f6758d7f3f76c383d9f59ded8501f25eff9be4a1e2de3ee484a2e8069c51e886a75a229ae15f"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 128, 128) #3
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"b68686b8cf817da9c93cfcd7aae410c02d3a8eaff57c6ecf990f20f70c587166292b5f56cef1ccc5018c38a602f811c7cdc16ed59faaf405":"03cd598585a3a80f9a81e2780c699269":"dc761246e0a74339adb76c729ec1414b":"b2936022922202757eae4e5d59eb29e3":"6e9735b82a9da2074f93b54580aeb76bc75265e525f1b50a8ee0d6851317beb64f477f3b3457ca9c120cd8eab6d37400ae62332bc91cab803b0c44e070666f9389a9d0fbe8baab9cc5c0cd54a397c8e1"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-1, 128, 128) #4
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"cb68eb95bb00beb896048d5d323d737942b1a4795806fc6bbcf67d195862172f49bb319e609965feda2937165b8dffa6560e1fd434a5ea0f":"700dc7725321a0a21a70ff6aebe30d82":"d57c3dfbcb18e280cef81c7118a520f2":"6e569776b8a26d8e7d3c87f99f932aac":"b017eb98c5d782469658d47569453b8322a8db7a2abe75b4e68637a395f7c67bee75a42b39def3aacb0b1a03677a0bb4d31257964f467b7b3962d912daf6d8441e5952aaa427c246a1f1a623a8498a53"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 128, 128) #5
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"81e7eccf46acd145d435b80f2a6e72eb1b236d02f12554270c26e8ba13e9306856d6219ad04a8f1be3fa436bf280f579c22b64c91ac700b2":"33a186afbc44f3adec590d7e36bd9905":"bcfd99d6931ea9df679d196d8412c9ad":"6dd61af0f5077df531c151f2dbe2bad2":"41e6ced34a97afee72166239455d82fe020f5464ccbc8e875e06a05875ca844d8b7fa3ec360d31ae57f53245e7c4bed501ebb6f9b4af350ff9cd86a571360804d3a34b9dc11eb4be6427f521bd14f893"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-1, 128, 128) #6
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"1b76bb8a0dc7067afa193bf5dae1cd7c03dcc37b5788d22fe0f4adda99dc6d776fa545aabfb767255001063ddd99c7ef656a16e7604c5102":"b06bb683dc5018f0678c14b97547944e":"87ea4f713562b129079b49956eb88abb":"5650ef281323b6acec34c51795c67160":"afeae028a358702743b14dd64414d3350eb1de78702677e30f7ff9e71d6f9b368c53e79b0a353a43ec06e9020c7234232a07d504c163d7a8a63496bdaf670efcf2597b66bd0dea2b827e0a4ce513425e"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 128, 128) #7
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"117ad3f68248555a2b9941cf0a56726ca162bf9b531f26e3416be004bcc6fc35be8362c6dbd9771d42bd6e187868d598f6e2647b536c9728":"16168c2a54d8dd7150cd7f122482a723":"4e4cb0001c

5288c1538dccb80be01e41":"8177c1d4def6bde093f27a9894d345ee":"1e407dd8c1dd1436064f2015eab9c5fb9b88b6dd017e1196ce70fd9ec878a8cb02e2d221f4096e7998dbffbf0b392e7f4d97e0d1cdf81755507c04b5a6254086b40d153b10faf0011980bc0911275145"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-1, 128, 128) #8
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"54bada0b89d9f5bbea78aa8c409dccd039acfd7b1645a0ef193b60cac97196e4cf9795fede9d898d082a9731a8ce2168a10420c5d6bd9a0c":"1c8feb149d98faf15b73622167064088":"a71ee8a522d67194bd1756c2e2898115":"669ef07679f336f529058672f861b0f3":"d72d43ff8704248a0d59a111b64128fa6bff265c52bdae38507ce5f302158be902d8380fe247abc0275dbbb502867f7ad1cddde0e404fd9d64ec494daac5d088401b4da696f47a31b4435abbea71c387"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 128, 128) #9
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"8cd407fc7a36315f1cfef1489a2ecdec433b2cbc1fda4ae1d967e192ea8942aecaa169deca4c268246edb421a0092a12091497a5fa159327":"114a4f3446eb3c98aa9c182d329b2856":"f29994a39804004e7ac50642f99c403b":"40782cf3d002aa603026e26d3bbc6dd1":"cf381392567f9e0d1f55c642bc64075699254df6b4b375fff8f869f7a10188046276dcf41076c55990b6b997db182fcc88cbacc4782347b9f4ce39351b77e378931d5cd026d997ab104b8b7787b2f92b"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-1, 128, 128) #10
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"dc8d705180e22f8be91aa4bd57a02caa30fe8340a53c64ad2d460e409c3a2db9fdfde9034a4c8f306195fa6653dc29d84d26af5118fb60af":"4b51ded198d1b16f80ba9e536a2a046d":"ceacb5b37ca76de240a9f4dea89a0389":"73c614b8e273ea9203683d1b0cb2d7a6":"6a136d4218255c70913b73af480af86cd8ccb6f319937e075365ef014187c312f9069f1fd05c6e0c44a1b7ba9dd25e948ac155461e425d864cc83b63bd84289b768058f7647a8921e23bfa7c73b4476a"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 128, 128) #11
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"1796646b48a2b982fcf7a4f49fee7e3d6be673106a4a29371eb8d3598888d53f59572c63c0e4bb183b17e0f67d81a11cc878ef600d1bb810":"5297aedbca866d1754c4b6af443ab24c":"771688574b52154837bdff6ddcf24d52":"f6c627bc84b2c01a9c055d4632ec955c":"9d1c796a2343ee855859e04ed702fa233da2f73ac9ad632fd17c8c5afe15c5600c6ab2495018f808b1cebc54b14ae2b1f929347be4aed9836e0b45dd2352b23cb28d753045f1ae6aff7598a9a1c350a7"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-1, 128, 128) #12
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"c5aa3b0e9d8f916f18e73daa0cb88a447f7510af40f9dd540f8ae4d62be2c5754f6eb10410c121388233201ff9c8121a36ae77e042a98211":"06c35c446e28f21fb1cdf2d40af53dc6":"41015c3ef3adb96edbfaea6eb8e0dea6":"e6b60016bb99415640506851c0fe3fb7":"027ff1ab4c406c048da6a8c24f04d12a5a35a5191b62b496459b750b10066cfbac502b1ac612b58527744f6ac5005d22d3f86c1adeb1c1bf1a26902474d08bf886ed5bb26e6d1b529df0143128b397f4"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-1, 128, 128) #13

depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"57c7e29e0305e6a803a568f47acaed60d13e192c1e16bd9bc50ef5ebb52c5493bcc4d7a0e5be64d064b735deabbf67e94395544497e4816c":"89199bb960ac741082c5fe5ea34ea2f3":"53b5b2783d8191ad4eae3ed87bc059ed":"fce4d7f5f0cb2115d4c4be2294deca56":"b98839a962db8de7a17d35c35bda06c4139db3933c4ee60bf1779b16d804d7c600a62f9c57cef93a79ff281989d90481db863d23cd24c4b566d74e1de6596b7cceefcef1f161e5a51d115128e0b23c5b"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-1, 128, 128) #14
depends_on:MBEDTLS_SHA1_C
hmac_drbg_pr:MBEDTLS_MD_SHA1:"567d3f4c0de396ed67569c070d87f2b535ec874e881418983ec42ceb295b7d312e715e46b96f9da5998f9cde45b1dc22db6d2d7bfd4f3930":"43c16ab49ca5174f907d7899ebd242e9":"6c0b479d9e847dfbeae230bd4601d0db":"0d5a2183c9f9ca6941f6a617892f5e47":"934fe82b0951b97dafc5ba16e87b0459691156b42ff2dbbbd8f6ed9b04be952af267c6a17fbfc86de91f9f07eed482a5362b176216a8963af485503ba93b2e82c03a3ee6225077d90cd961e24f6026f6"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-224, 0, 0) #0
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"f3a709bb47a36838cb998fb6986ff074c57932a669670570ff6cd1b202ee1da014a011f43fc02c51ffcb4048cc060763f2c58de2edd494275da14118c9cb7fd50475c66cc7e792406213a7d00cf7623d931a5947":"":"":"":"bbe3daefa61fe302bdaa6d4d379680acfd0d456b5d35f137c145b72626f2fcf39fdf7f3708d9e88c1710408a3d7ece3b0261ff538846fd5452149960215c0c22beafe6cd24a7c392d5845774b87528912c322119a2adf4d35a0ba61dd36ffc8a7e7475afec58ad4a8cf343afb677f087"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-224, 0, 0) #1
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"0f508c6330b9673e94861ae2057e200ae8f2b330b74634d79fe8a4c698211080db07e58b762a2387379f0c0e2d01b2ca40ef82fec35eb81a5493ccef709dbaa0b0e4494e460530062c8db7446bc6af2d852fd875":"":"":"":"583367bde003eb2061cdb6f51db9c6827cbcefbff0497ba823e112edbf7f2066fcffa3e92d1e8c531007783554e6aa8a633bc925690ca6d579fbedbf9cc4d6cb08133d0cf8d4c25fcd3b6fed95f00b1bb17477cf67b97a557e7da933bdc121481755f628fdf0f0b1189a097c7147169e"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-224, 0, 0) #2
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"9082871e73b098bbc58f324f12f6a83c321360c9f5b400d00a9bb865ef5265083d9309657c40ac94b579995902df0e2084eb4a6410cac605e482ea4abe5c8eb73bc63f68baaeaa56d47f7d74974d940555fd3861":"":"":"":"67c2fd4397af79297782af9baad2a26b993efa48c689a74531417ae102d4ea1d6a82cb0321aee3dc2572ad27299e81a7a77f1cf837119e746988f2ec60bb01eb2ac3d110a948c1c33e86833757e2670cc3947658f3b2d32ac59242f152e889d03d03056f0a265ee759d3a4488b55c63a"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-224, 0, 0) #3
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"4701f34326930cf93deaeb3a9c196e307a890c8ccf44a55f84593b3388a196238fdd97d201998ec734821998e7d6bef7b31fa2a81343918056c01d65f519c8576e4120a3d6b9ce28ccf57eeabd012d2c14e47045":"":"":"":"b499b86b0a25a0fc84a9a1b902972e2bb5aaf9b84f13804d6180491285b9316218cde0e73eacf722b5c664f4e618625ed35c5facbfca153cc184309754ecaad9c3678ce51ade96dfe3290e125d661e2afbdadfa73240c24

939bc31d171712c7c987bfb434f1db6ed44b321bcd237f149"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-224, 0, 0) #4
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"a912b6755cd2d677d63268a5203739b0785d7d956738a596e269128a583921aacbba1adb7c6d1714c164143c8f44e767119655146516802350684 76ab137d5962e5e5872f3b899d0e9ca5ae8fe71bdcfaef1d241":"":"":"":"0f410304b6d88e52c8d6039ca674a06c49a5fa1094cf341c4034e39990236d9e5bb8ebb6e59849e7df82e2d02981d8df21e4ba3381e606b99c16de62860a470109c0123c69ebaf970603f451f9e6acf83e1c5951c3cb87170ef319d9a791110aea0c0dae5623c287d4c454ec93227654"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-224, 0, 0) #5
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"54fb376707de02a1c385a3da78523485111a0a099066206f210ad848f29d3c270d2fd2f668cdd3a57cabed71f9d784c209259d1e4a3eee2046846a55a46965e495eb29725a86bd630dc43cd60ddb4fc93c59980d":"":"":"":"a2e3ab5390b5b79786ec7b434de48e45f590b85513106008479d8a3b7b236c884b0f871d8dee539c712509bd70de351f3881cd87c9cf77c1a9d8879986ff0f6678549c5c6acd15aeb6bbe653a9bc76829df2f194c5f6e8c7dd3058971ce15273a2d559c1ac60a0014e5e32352d6be2a1"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-224, 0, 0) #6
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"3a0c24b5a6106d28c02957538e76e96b3ececfa80ba4c7d01fe642a88fc822884cc36ac2703e8952ee635948715f78c542e6e3270f2757f1652474df4706490b18e649ffd95dc518a8b4259da193600af5d5bde1":"":"":"":"55dc24206aa59d34ea990ac6b31250f15ac056c8ecd52e159f3464c38e1f28840eec4c6423b0fd9971d11c5ab99225eda5d173c08f9439bb56eb1cc487fdaea934fa816f9c9e0d628f111cbe60a647e03892084f80775248d41cb587617671d99b508644476b66c1c96979e5061e025a"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-224, 0, 0) #7
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"ae7ff70bb69c964f05c99c0e7868210d567bcb5eb02db7708de162e6bbfd91fa17f30656420dad1ca69d356cbab80456cef922a9206f07d32c3f198c1a68e673c5583674bb1df1f2a69c554fdd3411c81a90c83f":"":"":"":"f1f3f79b1d7f988d4caf7308416f3d02371cc029a28eb4f0247c8625c4680a2dcbe9f3d56d92de6ee4d4031a254bda8a657bc147fb90c2f7783a8e3749b60633e5a921d015b846b3cb38830bc7554308af08ee8219e5acd1b699f1ac538930d257da4ef567ca570a7951bfb236d4d36b"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-224, 0, 0) #8
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"86704ad0286f88dbc60baebc2ed0571de7b5ab64bc8554ba8645557fa10159ec03cc9f6f299c1c3011c73b2563e571fc24f5b5b50b4bee514d7c808873ca804b147201ba7ed43430d89b066c04b00b0a17694523":"":"":"":"6b1a26d7d21308d217bc8988067ef3e21f5bc10d34e89937f2a89f8da256acef50b6ea7d9ea877bc1d15002b1766e9bc7fea3d681b147e42359ce29d6d4f8c73e7c29b9ec14277fce2f6a0c518d24aeada44990f7f92b0d1184ff96b20c76d506f6f9d963391abec5bc247a2ac6b24c7"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-224, 0, 0) #9
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"d0b30341b4fd48281f76a83d7de5769d05d5cb9e565b213c8e2bc8d4adcb

ae90107fc12fc1ed2a19f20beb563de8f05bc5c437637148154a12b1606bff071dbb366458b74a07a1c14114fab487772d436d4ce159":"":"":"":"fe2a7ced1965f013d475724eaa7d31b62740be411d899afa79f9fa6e73f18ebe0907f2f21388b6498cd365798f27f882a2c5c2744a9b25e8d351e77b9fa4471ceb1dd6c72fdef75977e4e4a246e24f56a615189e1b2a8d6782e8c5062b744a65ebe1f7c5fbcab333fdc155bfee300503"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-224, 0, 0) #10
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"4a1a697e41537f28b381e05f11ebc905bd66c2c1d905d8c0b78c10c26cdf547a1b6f85ff58f48298a11bba41e3ec015d41a24d9e335e6e13b06b84b9f56b3e803bac569dae2d74c444bb58b3a6344bfbb9eee765":"":"":"":"15060b2bc827dbeefa2170ade633b0f0075a4b9b03fc24f73522174be4e4b08b93b421fa98c7c5a445c3aafed47a2eeeed63f19ef4f67e7726d8ff84bd94daa3338e397d52abea4c7d1191e30f3e8a11864f10ff56b2dbefd860655d34cf63ea22bbb54dfd0c5f64284c303a2ba2f49e"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-224, 0, 0) #11
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"e80b8c8896557d596e192c3226347c336dae455b50bf32a78c61b9a98c949096be51538e293d338a464eae0eb18f1ab21f9903d07a8b98ea2ad7f41fe7ffdc4b4bd0fd06138a84dc5217cc8fe39b92f9558aa619":"":"":"":"55574491d07db3aff94dcb71f519cffe2f96ef57219262860c3c03f9a5b8a1eb88869e69587f8bc0693c9919bb277dc84fa55187c0dbb20101f0c4e301dcd2fe21664e5a2f0dda3eb4f11df3878c5becddbfc3ca032a17f740d424b99be0a9bedfd99907229ecccbf459f5495533560e"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-224, 0, 0) #12
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"5c25f02bef1f1319cb6868d836c9cbc182fd8d86ecd87bc5cba41c163710074e80d1a30ddfd0f5d88c6682292cd50c68966d15e6ff95e117d342d974ff074ee872719d15745da624f8503a6141b0ac4b887ead5f":"":"":"":"9c5204d5471c25203f1d9786d38f71081a872f1c56604dc7570caa5439f17cddb7feff01cadaac8e0f35e7a5433cbbcd2dd4f11cc7dd14f6af629fd72a3145db6924d2bdefc262662367b7258cff36172263460f4dd52dd08faed3460bbffe18eb10ff5b3c6a97faddf65b3e21ecc98c"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-224, 0, 0) #13
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"68b4e1ddfd16a1c1ecb0f4221306e77ad02b07993457eace086f66566afc5f12489633c605d11d53916eee96ed778d6d6518c5681f0fa9b0160da1c71740a94ab33310bc20a18710015af25d3d667c40dc619f34":"":"":"":"5c4c9b3276d546d3b6277a3a2089d4969146d833e0ace3e1ddbd9f79fa2158531f8bb26a28b08dc64bb1e610f13eb14c9fb23559dc2f38326e145ab509b9f69259a0d1a32f471d5abf154a2585288063845f99306f9bb875ccb0d32e9d49b42900257ebaa532e8ec223aea60abc9714d"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-224, 0, 0) #14
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"d5ee5e2e629ea17487e593914012575daa8baf2d0e9671e1b8aad16524dbdf7d04c11130cdc10e50c630ccb235579a72b6eb4502fe146aabdab62a085c820ea46bb9091054d75a892a83c3850da0a31c15e0d021":"":"":"":"e32c0798b2040620fbc5d2a44ec7fa8038444c1910fd4a24312c8c8eadb57a78606449cf05ac51a3bc4d58ce78742c1be3a0fab6e3f5ebc92b82b5d5d64ce29e8c2787ace0f4e718a7f6cb669a0a43ba1aee0d9aef55cb7c6f5dff57c8acfe883ffd8a496d44afe06803e4c9ff62df04"

HMAC_DRBG

NIST CAVS 14.3 PR True (SHA-224, 0, 192) #0
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"6e531842b9b7fe2c0ee66899a1255135f784a2d5259c93ab3d63a5cb708e2e6cba955897d9b66c7fab274aa388a5db69713c86faa4a19709e9aab04638c670ffaa83806abf79a43e613e62cccafc637e1a1c0c14":"":"e628db057250fbc6fc5aba01b6c8b47062ec5632a8566730":"bd12e61e3d5218efb0c103dc49402800cfb863ec8925e76a":"037650ddf66ed42ea38cf44aaa94884effc5f831c593fb35886b5d601a58f74f868d89f2dba450b9c160e28f69fd24e30fb7a44189810e29afd0d11762d3ef07b4527f4134d6c53bdc9b024cebb6b40fbacd68b6acd4bb4d011d6705ce22f90d910ac4017d2426db7a48db3242161aa8"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-224, 0, 192) #1
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"3fadabd2d8879bd2298f53c54b573db2584655e08a83289cb58a4ff5170fdc30d71bb24efbb5a50def315dc69146111462e204289a64ce72767499f299c74c934f0007ddb34bf5183bc1e5afd8c15eebdebba882":"":"742f7022892c2123e62379e9367787302fd18dc3835de0bd":"b60325136fde7c858054983a977262b6390a48419725febe":"3bfa419f9bad259b871703681284c5396fa94a323d646ddbf5339398c4d8314a999c230894ac60bf231762acada672f58154a86f80a8c4e3bbc67132e22ef50c0377193cb0d13c7e2c97cb24ce5bb69c73be2e5cd3a07ca2b000b2d7eea940053156bf55d846181e3748a91c342e191f"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-224, 0, 192) #2
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"0784a499424dd1c2c13f765e9ed88d752fefa83cec61154f82b3fd645f642ff103db9c8d1c10b5979c56a22d58324669d4ace3994927222fa87fd049558a48adcbd6ad5a2380d2d927be57fffaae037bf8a34384":"":"9f853db57c3da0421914d2f71f9317817580c1de4ca43d50":"27071ad475b8541c1a80234bb2d110637fcf4b4e20e06a7a":"2c879a03bd719595211b526101fe85702161711c67a81184cc42c1f9da5761e853ff4b8d19deb95a2f3323d1cd58a2e066c66e7a30059732eba43a4bf3b22fffa5bea5161fd775160dc53d7cbb4c892bc122e4e0139f8f550219cf6fbccf55d16d8a4d8d7776aa143c00d9e7bd1c847a"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-224, 0, 192) #3
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"addb36bc9ad134c7b8fa54881db1b18e040de4f253be28efbd36b12bfcf4721b08c5833eb0a97c668c7adbc7f04a9e0299549126172e25b9e624282c8e63eccf358c0ef1a71f8fd0a8fc49451db7757eae344e48":"":"e32540418ef68c3dcca1e7a0546e5dc7d4c5e92019b8cb0f":"327e31a0619305c93e9b5eef87102d447d21e21e2d8c1cc2":"178bee4059af0282854c833e11e7bba923a1e2f1126fe8cd7e1694602c180802d67b845a88ff786147f22a74e6ffb0f8b86d352cec2714ff8f308b1f9705603faf5b04bea3c75c87c91d5e6cf7583b5c45eb5f5a74d2bac490c8415d2fe07726bc334c88e3fb7284058b006f82e89ae7"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-224, 0, 192) #4
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"412431badcf06f87551ec63c3860baf4b59667cb4753363d0f82fe7c968ea6f8bc5d015418adeae206005725dd9693af6f7060a2d5ba53f66dd49dc148de581737b67acd4bb70ff2f4cf20abc001ae1eb50cb75f":"":"d67f94a953e7e4e4bc0cbd517f963e599d68851cc333644a":"385281961ecf2d8175c0a718347d2132f059964c55f39f57":"357876e78a69cd4bc4e06b2c52ad28434520d54a4a310ee0eb026b87993514ba1442e25eb1ae22a3ce98529625d8db9b0e5b680d7e027523b0ba0184d3f2e4b9cdee027960ac1612295bcdbf570912ed05108541b97e3bb30ae0a122d74cb536e5db34b7d5ee5a042897d5d29fa3c126"

HMAC_DRBG

NIST CAVS 14.3 PR True (SHA-224, 0, 192) #5
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"ae914c3d74acb6e2d9b8487927db7992b838ede73dc918b60bcc94f0f456f454a6d100c90e119342154bc3ddb059f48db3a8d7b7288eb42d0ceb07532a2a357d20506ead28d9bd4a127d437a657a61f5d30b04cf":"":"2afb537c13fee9c4103cc6abb11225046d94df2e9838f73f":"6a9f670cb49cd9ad98a17cc19d00d4766344108f0c86804b":"2ed0c4140420c6e3798a13f917cd998b2ce6f98bac27f0fdb09e2538f573caff16904edb371f98f50964b7de552e997007fcd267b36abed12cd95d9a08852a4ca862872edd32c707e7a60e11fe0a7db4c0d34f4c70ff16e5c75e6f5d7ffaec3be383b8790ef0ff3a0d9f79850c9749c0"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-224, 0, 192) #6
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"38a93c3ede148c91eb7f0cd327cbe8b27ff0e569bc5262aaf30b86d31be35f83b4ff50b84b5dfd649908d0c55cd5be7ad36d4f5f7f22cce066d3b589adef804bfaf52253a0e4c6bb03e000d649541e523ae52f1d":"":"e12c05f2bf463d24da9abe89301d2acefb7957dc1bab9ef8":"d70065fa713e2d691bf554a00d063222755e7204a3e53968":"3e5ad7e96c8cee899889640d8268cbea296aee96fca7bb60308bcdc08eed36bdc8a5b3126ed8be900577e60ec0f8b3d3014deec41ac650480e08dd3a425843b37fa5d1d621b5053ba4b2fc1804d407849a84e9eb5bfcf94f27c2a535e2756b8202ede1f18e81f65e3f7f51a064b401a4"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-224, 0, 192) #7
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"384d6f43e7d77a381bc6bfbfbfe1a17aa35525bef01be8aaf6c488c46517d9b94380c73d3fb45a4f1b4d70375021c7df78eadb61df5d9efc6e08fe2d81ffa65df33667c23e3cc5c89893988f04be1d3634ced443":"":"a0271fd2552e037568cc857a60a550db050680fc03904fce":"ec095cc9e3bc301071a901d0289b54aefc796bffad6fda8e":"aca2571a9cf6bcd10429e146e6e94d1ae43a00db28bee2b60eb6a1bc1cde3d452dd6e04617aae7a3f813feaddc0f8fd25890004607f45ec995df970e1a3abb17b416bdbf62b6ba5625a80cb100e2b87260a73ffe15d9e6f24abfe9e6f9ba66bdfbfe71380d832418e2a4b460dd7415f4"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-224, 0, 192) #8
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"98c8df867d234553e504fcdf807fb8bba51d23ac65dd8b160943bd45181764cf6df0049cad23e6aca490db57d12dc6c631604c943f153927d6d04af042e1da1b225eb8bdf4ee99dd405e3586acf8e44bb0184d68":"":"3338baea79c06f0d48ec2d47004e61c1c1e5056bf8bbecd3":"79007bfce109a682b746df074e87c845eebd665532867fa2":"ba7040193e38c4495971827fb1ddb747ea80cd0bb1fd6aaabf85ec1959c29eba8f818ef55aadadc8c34b6a7c00f210a899092b9704f2e03abf3e5e8fe6d127cac0436441d0a6f1b02a00e5fe948539c66a8c78e70f35cfeb600e1cc68c06553f47ca053b64a0534a028a73d0890034fe"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-224, 0, 192) #9
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"6150b7280b3105b86b66c2a39a1f0461cfbce17e746791afb241b298741454e174650ab1e7f08500bd7eb096e40d8114e5a60668636b6ff66d2622154b7d239eaefc9ab2aa3351eda2af4fe51de36e22e70235fb":"":"6ece8aa447d2cf51d8497e303c1a202e39e06bd723c847b7":"21d890666d2c8ce4440bb453f4284c3928650f8cf38576d7":"7554b8cc8e79330ae55575f9157cd10d8eeb58af30eeebe9daa021f4b55ce365fbdf3629be7547a89c78bb9df79d35179e5d2924aa032e60d5a00281f19ee2255c17a69345ed86bf36ecfd694be0405c8b6c077b43a8c8bbea603ddc632a1aea6771a6bc117dbdc365e2714bdaa8b377"

HMAC_DRBG

NIST CAVS 14.3 PR True (SHA-224, 0, 192) #10
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"cb25eef7230ac2da249fe30ea94d3a3332147022bb2207aab4a50822b1564c24a047ebb46d57f45f6680f909629b43129876c75381e3b7c6d06887f68083fc423f06ecba159a90edd394cc0ca9473e9cd0f23c89":"":"2f30b005ea5d5965439bf15220b1c010e6c79306e700e6fe":"9937bf3edb3603cbbe190f3616b021fad652011854e6f6d0":"040a30b82981f71e4607c20c1f2d6e6854824c90b127517f65b6c7da99fd33dee32dc52bd0dbe902509c50492a88e5963b2b6e27d046334b356e5909f85763af2de70e93a89d6a00e2ef81ddd74f4a33d3f8406d05b383fda569a5a574fb5e3c0c86a5096e94174b79b2a4eadebccc2c"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-224, 0, 192) #11
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"1d7dbe4e83913bad3fa918262ab0f45cdb9e4e61667694f361ddecace06bf352b18dfab4c32bff9a013d3b92a2da8ed698168155ddc492f8ad5d65cda8eed212793cd9aec8acde7e00f952bb5d00c53c5c181e89":"":"f9c51ff8f264cae722734502f6799e4fc5bee773d31e3e31":"6a171a0a8801017a1d924f80fc5d9d6592b8b28a342f30de":"425024bd1d1a66d4527a3e8a8307b3206923bc1d693f5b7f9017f0d5527cd6591016758794ac89e2f682cb2d66f8d28f9a2f5ae2974a75f4d0de17dcd02e93bf29c69175fceba262378bafbe3eb7e3dabe974889306d0a2ebd0ad9d934c37b1ad89ac1fc28493e6b1f6f24620e40eaf7"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-224, 0, 192) #12
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"a6887fe41ed5a615eb030b31b86315d32d13dd5ad506566ea23ea3b162b8dd621129736c8dde31708a7fa4a4c606dc212b3440617111e94a5c6722c3a729d84d2e5858c23ba8bb249456a11d63dba9d4260a7213":"":"a52036daa8172111e89c8991ca818bdd711095a1602f2f15":"cba427a2b7bb64002e1da3159d643e002516bed279e0d442":"cf0f5881032606c21a8ea20adba6a72e176e968f10b08ab6d08f997b24fc2a24f2c5d44d1b99deb7db4f388dc8ac268f966a34c857cc5f43efc601674bc548ffeaee1c13415df6d0240835832cb75840b60711cb636f509dd9b87b698615959688e9afeffa50671ada05faa564c87ad5"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-224, 0, 192) #13
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"a563459889ca29b711086adfbf18f284fdd18601ff69916af1ce47510d33f205d4dcd0080f9dfedb2bc1e2e60fa0b9cae094102bc7a705cc223279e0fc3b0020b4facafc2b31b9bca92382f3810d5a4e3ef626a9":"":"5fc83f1f6dc0ad454bbacf2df366c803cc1d2fd46bf78d32":"1a9654667cfd6ad0aad9383be04ec1480a494262b3fee823":"cb45ce96a973728bdade51f91004ac09e155173769063b3fb4712493d8877f088127a3492588e99fef648a101cf1c238fdefd798dd4928b5bb3a851eed693f37d67360a28a2b27c4406e9ddefdffba662529b91a980bbe4eb381cf9734b336e2b64e7482e0328c2e2bf81e39edc30d97"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-224, 0, 192) #14
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"886d098731abf3140d512e0d348a384d25372667fe7e4f0ce713b1d2eca7b2ad939b25af03f78edad75bf0ab95b4110710d0e12e714e03f7df35db59fc4ef2906cf36c6c8897b802200a83e60d16f7fb064abd2a":"":"a4f42d83a492db3fc053d1275c6f264706fa932955c3da62":"4505c0664e59bb4388020470838bb098c4ae1338c268adf2":"4f9c3c60ee32042735cc539b9a23d04c2bc6bcd68db04a58240305f165bccebbb98e0f4796b283a0d78bdaccfcc8daf19f21a72945be07996bbb0b606643c7753f76ee6371292d3e681468b714e16bc32db14ad6d777677137ebd3731186ea72b840b8c4ae79ecb2c61352ea056d2d6a"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-224, 192, 0) #0
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"a26af93571ba84b58e14e921a6bada73083ec17f21580a152703e1741392fc9ce6046f77d6eda5000f3225ef28425e30cec138a16b0ebd885fef074c6da2a7b126fcd1f056e3a5fd5627368c63681cc10fbf750b":"0627d10b1e5b4f0fff96d0c7e684deb9fb6a4e48959dbc29":"":"":"98d6bc7ec7cd72da4c750d9173518a9a17120fe9af10cd1a7d872fac505d9276c551b821a868cb8b4d8b10eb3b05845827717d2975814b5080a2f4aa50c5b112bd01b8652f2d1b56a88c6c891db5f3f40d1d1f0648d84e6ce2138c2c879884eb4847856198579eac759a065a5d384c46"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-224, 192, 0) #1
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"5fd08930ba404d13a7275227660869e7eff10e103548e6ea15f0816ea93b649f6aba408ac710c49eaddea0b4d1e219577e6f6ba4f193386228f6fdf9cdcc50d5bdcf6d1f249e9cae0a097bb341e2ba3581a3f2ca":"7a463958302109d5fb9fef1a232b5aea13ba58a60b70911c":"":"":"a1a5c9d90f9340c807efa2068c6a0b872a4ad51a7cf90e14b4797dd894361712fc9507bd61d8ba984ecf1345fa3cbcf3031e2bc4302354cdf3f615c3a1bf43f60a464698e250726c37a7a9a23e1ff7e8d96df03957e3a0b5e6c4c4fdbdcff487e467b12dbc21e07eb8a7c4cd7f779912"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-224, 192, 0) #2
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"625d6a509ec43c55bbec45b4244fa0bce24c74cc270851f2d32e4bb4f1961476af40088b5ea81f7a86efba78abdfb50be09e1a68851899e0e9acd95f77f16e8b0aea5a9bf29bc1a18d32158cf69c794f3f47fe61":"bcfa259c919f6e56c77914a272959cda6d2cafeaff87d91b":"":"":"b5bc1f03099547ce1a359bede1f9f3b76b38e8b9cc781fb3909899144f4d0a4ba93272552bfb0ddcda51165d0ca3eae47d10961a62692bd9edf2a9339c8ad14469f1834eee3c3fc1074cb1493054f84273e4adc73e5eec6cba284c5b7fd8005f10cb67b0fe16ae0b4ff30d50ca245c5d"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-224, 192, 0) #3
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"bc0c83de31217ff6b22c719de8c6653fcbd8aff7925f04624c76f586ed3bab324b64fa8a1ec14efa8d8d0b41eb6735d517f6c647ef8bedf3036a6ca90fa1d2c528722de33f76f7375711b6b4127b86fe096e72cd":"d7ef6b5dd09c08437313871078ac730c2f85a5abae6d6e24":"":"":"6d415afc0151c3cb426eb3b90c209feb726c01e28785678bb0b8d9143d4b7f31ae07e384816072e2df31350b133a8f4e3ee18f04b154d194513d9b072a695e52bf03eeb4c9a1df85dd6ef98d2453dc39390bc3a17f3ce499d9b182c89d0591dc3dbdb7aecb626b07f0ad2737bf8200b2"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-224, 192, 0) #4
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"caca2b8631502fbd8bec33e89066e77b97a57b09d21a92dcc7b65897e50d7a312f287932c529f6a6fd8be6fad5c467f6c15f9bc0f39653a6e4963c0d4c4baa9d6ad39f4ad2a1d6587377ec3898e63e02cc0c454f":"33691da7461d3355659c4ca927b4d3e3bbfd8e775b535538":"":"":"89abe8e656667299705c4c8b208f0fc400897397d15aa3574cf86c0a6415dd30ac5d7d8bc629d8ba52e6e5af63818475874266e98a43ab5d3085d2856950e8d487ea22e01f9ab7fe1862be1fdb9a97cc24eb9ad05beebb202716607e8b164cf63cacb92504e80e68e641af71ad6ee47d"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-224, 192, 0) #5
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"5d97de97d6f81a858ad6ae0262e58169b27c25adfc2bff506854e6bfd37f3

a4d8c4b46cd78d0a76b0dc67e0d3f90fb04c2131bc31239defc8eabe9be0fc589a554a4b77fa79c64c03bbf87a3203153
0d99bbe397":"a0d8be30a0972002f21ce2d7cf3c8e84907c638e0093354d":"":"":"67536d7352a49a1a49110a1dc1b77
dd1924be34123e027aea0ba6064ae0aa051d4470ccbf923e0c96c86f2d440f17f45b67c4c7785a6f5006bf0cadc132695
40b2c59bb75f642e9668feb601fc60c18b94d65ebea0dfe5fb284e003a58837f9e9e120481ec2ba972c755c6a9134af683
"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-224, 192, 0) #6
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"9ca7149b0c5ccb7a0f7ec5399c644dba98c418373460c59978d91db57ff7
14897ee71caf459c1dc164655140810992fa6cbbb708ba2e61053d5866ba6a1bbdbc639fd21be4383beb4a4d370e86d0
e9739ef849ae":"2ade2ffc19de7fc94767193223aa1fb3461cb29d970c8f05":"":"":"b39d6db529fbb3c6a90d6b705775
9c26a9fa26024d2b65e3bf459881ff0f88a5b93b87e0779635022cea81db313329b61613742cc82b52fff1a2e6e24ae0ee
bc0917d5e4573466e4aee3f0ee0053445566eaa080c3e701bc35d40ce5105b4b6572baa7b4c84a16e4aab501e6ef67016
4"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-224, 192, 0) #7
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"cc751171d828dba023f430b3f5a7134f733f4cc1ec76495e98a6dc2a627d9
7924716d7e6b043cf15c62ce8da1dda2a930c88d6d4d12ca992a501f773dff5d38e42f150f1c55ee358aba1e73cbebf465
baf9fd0a6":"4ba50a75424970526022c7351831c58ee75f1e3aa0c47749":"":"":"8b387e55b9c10d0cc336f5445755c0b
6dbe971bf69a04682b21c9303a66e093b7dccf33fc685765c6d2bcfa3020892ed09ce6ea3e3355b3bc16741f34d40b5c9
6bb085c1574801d14b4f71c97cf64e75dcc330fafa1d1e626822609a9af62c894dbdd56307ccf1ebbb7ec09d500096aa"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-224, 192, 0) #8
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"1f2ccd29bc38e8364a4beb0e89984b88d61dcd31d48e310ae691c0e146f4
95b9d8cf443ed12f3ad2da7c59c2a2f6b8df4e0202414791e106c1f879879b7a46ac207f45b5fed69c38309adf15dfd0dd
75742c0df0":"e0c49aee71c4c060aac1bab1f438f9e2b0c96d710ebfef77":"":"":"593677f65ca4339c0dd8b1ae9278cc4
9adaef1cf889760b4631a379d82bc25123dfd2e1436d0b6b890d4155e3236fc1e2cef67d8bc0454099051e220d6925b3
7c47408fdacdfd54cab7be70f8b3b3dfc5a86f181dd559ff7182f225f7de87dd8bd69143be270ce76d2562c6e01ba4c4e"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-224, 192, 0) #9
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"f1bee9caecfd0397a6cd76f356ecacf1053981c64d315db4a51a244fe3b22e
f997392f65dc13cf30f5b8f5edb7f8f55863a30156722536d02440e5f06e503795d2401775a560685f2ad3c98aaaa22726
cd6ec45a":"9d42670ea4113ae02302cdcc660b497f3ffb19b9aca8babf":"":"":"78f31a24cda43acfbc4db7f17c57805a4
b53353d668596247358b47e8f8deeaca312a7f9ce78832bc1da2d6b3727fcb847ca4feb1695a2edfd2ab24c486da125be
1c1af4f78b749afdb57f97b4a8b892fd87228f116ba10fa739059581256de4fb865d1115c58284cb9850a24e5b7615"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-224, 192, 0) #10
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"17b3146ea3ac1afdca446275f3b7539a517766b90e2da2c4c85db4802943
efcd8009a9ffdd054440da16edb641a050fce3f3cab3d5f03d550111daeaa8841a9c814def76eec9c4e910788c71056242
8a39cd0987":"f3831c1bc859fad452a76ce513575a23e8b790c90de4575c":"":"":"c6c85936cd52b5271a6e70410e0b9
d960d76f3236b548cfd4fea26504ca8a78e58ee914c6cf248f30d7ee3547eedd3a4d9869b15e326c911aaecb7f0c221f8e

b9208a9b355e4b1cc7926380d25bb776f3e89904943b3fdf306012fc95d06b3b7c44ef55c9eee675150b332e2181f2a32
"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-224, 192, 0) #11
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"fabe526177dcd476be9950233ec56f9122a9b083e589c9264add302d4768c06020cf53e7708bc728582360cbf06a18de38e3da2642dd6751aa686dbf11734bd75a422571c9f2420915d7d79d9efea870e72d262d":"ba5858340e6a82b2ecfe1190215bd8da995ee8ef572eed8b":"":"":"10260dfc2f2322f530192e96a2396694dead62f9b206137108666cd199939184503da75598f54a89dff885a9856140b56687347c2c066a1593bfe02b8bd2cd93e939c424b33683a13678ba5f34df3f2f5f50b2a708d1d5a04683db00a607e2f80e5feb20086e3d64294e9732b0776c51"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-224, 192, 0) #12
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"b7c9a1d221fe10552bb0b799e18d12cffd1f76d6a1e6dc79a36584ac7e13c355b9323d0ef2f97fc2d8a26e6c37209a485963788aeab084e923a3794c63713c2ee288ba3a99f2d407adfc1b87ba64fcc5a7f98e4e":"e563f8c8318862c7117af8946823e8570ebc64b3de1b293e":"":"":"100c460c12e5ab12a72bd4351f7b608f5578060b262f21d735fe79d13c942035a76f001adfd39fe93caa22b6274bec282e640469d3f454d108991a1b73d8acb3d392732fc24cafb15fbe248441462bb2c1278883610ba28486ef82ec2ff3d20eb9601866c7dc4eaf44cdd73e5b5ac14f"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-224, 192, 0) #13
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"78e5d4818964d748282fa8dd386ea9c920c4fc5ddb9d2204a3f6285082b8065dd3944ce193722e973f8300783e37991e6c4a6286a1a0fe3703dd78ae951c88a0ce47b1a23d91e0926358221713670a78732d5470":"fa058586d35f0d74d2c473e005e7f8ddc33a1f6d5bc79d75":"":"":"6b603b098ca74b7fcf3c8f9b42dde5b3b51e84cab4f67f4d87bc6575ad4fa3f1e0ee27085f88e2a5ecf4f57f9ba92638e52941535806d2cd1b5aeb5b7c81b3d44d41cf5b8073b646a9cc1b0a9f7e183b082e9f2270acd928623e8a46b46257e1b827e8b88b55c88a3a3a067cfcb9b2b0"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-224, 192, 0) #14
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"50241739e3f08c910baea7f9ba481511b6ee5d69bb1a2dd34f3987a231cc25f39a1a966390e391a33dc21281372589e2a667cdbbe4267710d5244fd342c959b7272b39e5cdf67701d47665b61782541e94aa224f":"6a7d2f2dcfcae8a284802c97d77917e87c6cf8417c2b16bd":"":"":"4402afee12048c1c6a44624d2df026798930ec732884899ffd20d17f1c8d7c221cf5edac8679a21ee11b177ecfd61927d4ccbb175ee6b49cc6f371450904c2666aaf2e6cb36cd55cae3af772beb80955cf67b4e8be1fce11250a39693ecb7f8ac05aa23b949ac74bc9a67060cd60cc77"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-224, 192, 192) #0
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"c3005cdc5c5b7b25ed78c9684f3faf6278f9a9c5a9fb202014a29882e50b21e56ec8b7947fe871daec2626f32372123f44a8721ff4339e0a20f978ea27609eb495c2342e9ba719bbd2b44ff503db2322ada1c982":"c4506109937e0f9352fc881b0396b0a103626a15addfe525":"6ee49c76d138eaa3fc10cf411e0b8ad5488d77f74faacf13":"8825122b506dd6f3a58811fe6c9a7e9271a6e68dcdd590e2":"e818887ca1c84717e277baf00913d65ed58a8f90b8728080a03043bb2ab53f55fa605ba0cfab29b4cb694f6aae6594dedcbe6f74e1f7573c2944f3703b89a52789b

0170077ea8e66d8299ba5cc139943ab96254065a27abca2098a85162fb01d294d8671b00206b7f784319384e01b3d"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-224, 192, 192) #1
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"9bf2ab19aa7e9ffc3461522f3cf85b3292b54bd3e1099a42dd6f5349d169d59a152b2dce675874b665fcff802260ea84b358f6fcf8011b511834e8447a73c1f675b7598d836dc9fbf40f1dd0f481f47f95f3ef4d":"38d7a2109c6fad9205abc22b9ff705b7f671c4bde5b662d4":"b46e928cb59eac0cbed65645767e96fd824fa95cb96a1cd7":"532c8d3748205cfaa826fba7f240e9926cd3811da8fd1a5a":"bc367839d1510316ac3ba17fb7bf633a6eb4b61dc0b03cf1cca564db8248ced0b47ccb36e730c0237b0812af30361b5dce662636b23f87d6ace82cd3e34d45a1133b35ff9b8bde8fb29fe82298820c0c87f0e30887ddb15c9644bfb12578f0878a710771ad22fe16935c66681378f5f8"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-224, 192, 192) #2
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"a3bfbed559c396b807ffa80409fc4e2c23ba952f64a41c07d3af5e5b78d8ef88171bd5022d3e02efefa644f4fddbe207e59397605a0408b0201f6a882def64d973c0714555d2c7e0a6fddf49558fd1328074ca79":"4c63bef79f71fa82168928619cd09b003aeb2ba2b04150d2":"c85bb368a82d57c70cd5ad6327187c8550f7c10380b2f030":"5d467e9c06ee058ca066dadd6f6ec6b0da59ecbaa4ddd12e":"1ce311c919c67e151b51ce3060384ca95c071a295f01e54349abaa2da8ef497ea1364454133d20f57da28985bfc6d1d2f58f84d144c85dbe3c9fd5e8958ce06f2f5ad5af7e16bf90ddb4a1e2947f78008467fcc38b5a082eb1612d68e36e3c0abfbfb3a321eef3754ac16c41f96bd635"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-224, 192, 192) #3
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"1b2c2419e85386716135b3c142d749f1f5bc23edbf8c0a1c53b72f474484c545761b21aeff05cdd35621d104ee393e791737c48c5a6e6b25b58c5c5be28ecf17c410c9c9c3c3aa2b6385f66759f31b61f9fe0286":"b69011f446e50880a15bb0dd00229f765bf77b2a40040109":"67eb63a168aad8712a0e7e0f162af7ac7893e902f1aa72cd":"23bb752e6232144630e3d3a6daaa1e58a5ca315f21fe1d8b":"cd8e6c6b8a1f7f98f5d796023fdd4f1da2d72eedb96a8e85cac661da24dd0a7810fa04be0491c69db7617712582b43ec4bf112d9e2932288f25b64fb7a2a09ac8747b8f71ce75e3c80b854336a0457b8013ec6dc1268b4c7e8f7d3422a4a5d432f8d9705d6a273a09b9f9273f4928c4f"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-224, 192, 192) #4
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"62d059e3ecb695167e93b3cfd77f96e681985ab5d68f15473a89f9cbc4012e1c090a5a9e65f738be938f44fd6cb157fd9b737d9389e4e56b6903d4d015f9d80d96336730fdf57787296d447ea91de7e686c7a81e":"d8f121b2bbdb8530c6315c63e0a52e383c163c033d3b0854":"830e2cab11331b761aed55db61681fffad3a61a1a06adfec":"c7783d7357ff30e88cfdbc90569daf03d3fec8caf89619ff":"e44c9b35d3b847a928748094ba6754d1c5de3cbe3d90d4e2bd0c0f19dc5aed7228c541044b2b14d7e67dcc148ab04abff7c22a8f1fdbec4d68ad24a7c4b0f0e507bd7f2b4845593363da484b481906fb7207844597238b9d40c14237004e275572aac6a6d84d151fa58abc0987e54e18"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-224, 192, 192) #5
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"fcf3887b4505f7a1273ad5b32e064ff51682bca23ed974ca981871a5b7f63e5ceee58131f9a01fa7c37ab14150c9323a03f694e463496c4159eb8e5d3ebc62f41264beb93098a42a3dd406b983e1fb040d108f93":"9b3e97eed077155cf181829233868d27eb773c398575dfb2":"75a75a15c622e69eba698a064b0b41c8bc80ef803df0f29e":"7b6a20a222a81dfa6fd164def816c2b6708bd4c761b2bb8f":"0b3d501f728d2f1d8b0d7dffda0160157b30d0d97932315f77022d1a6fb30d9a0ee4383f2f63377ac6e57b16b0c7480a6f5dd12ed3ec0bc6f104a26c86592daa

3f68a499570703306e2c2448e784b67cd6efdb4ae64a2e8ffa5929e74c95b663c9b7fe891633f07d7b50f5f16e9fe567"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-224, 192, 192) #6
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"7a6a0774f2cb5ddce6b5242782fd3d7b5c7c7e31cb5fe95367c06f29a5488fa37feb34d689c646cdb162e258ad636a030ff74f6a7ff876417fb08f5c5decdcc98692538bebf9958c627ad8287633f98c587cdaec":"fb16aea72967c43b8803bcdd3e794911f6d53f2cb7946cee":"67d89947396322ca243e2c591a3adc8fd9f1ef448414fca8":"a0d568f4fce862e5e1b22acca29e60d7bc6cdcf6cc277794":"758b4685b0db1093eebde07ba11085a9dcab64c8d5adacda070fd2b292bec49240f25e158fc96cb1d0ecc9ebcccc360b981d140e3cdba54fc697313014450a9af29d9d55dcbc5bb9a38e4f10c6a3e41874d5c6688f22d0c5714301083cbbd0014880af0f7d088dabeb4e84a64f26d2b9"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-224, 192, 192) #7
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"19bbbbfcb755cd9dc000abfc03343ef64193141c3d3f43120f55674616e3d96b6086adf47c906981923c98ef7dd0fbb2f7af0ecbbd2de848f2b25cba8651b7e3aeaa0c59b605e6d4710a01406565ea30d0c4f68d":"e77cce9d26d283bb5d6e8300ad0f69df723324d23928c6f7":"0586c76051462d0483071213804385d01a07bcb27db05e06":"1c9363d0b3e9f42b6c722b8d62f9c633066587577fe766e3":"6d458079264d5f3940d098aae092690b7d04cd46d6d5dde753063b7194118ab67d3848459156b8f0216d85b5c583a1bfc000e68111be459743175fd114253cc24db72ecc978ff8620301ecbf18f42fc4697d91150649a8254a9850d5c28f9c4e187e409e496e2a659b2e79c06074c5c9"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-224, 192, 192) #8
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"c2b577bfd802b8f599ca14bdd5fe5003ee28ae69ca5c246df4f62d9e21a7793281c48f73ffea15f3c3d444ba48367fde04cdf6d62498b8afb24966a8662461015135cb55034a63571a032d3cd2c1e6cf4a6855ef":"f0de29d4530b4af75b8defe9b3b24dcb7ce0add4aed6f72d":"90ac05703a8e0c6057dd2d8b1a6f16f0059e7c70679919df":"16935f700de9fe529a2bbe811dccad430e27dbc60549c3e5":"56988f9328a91314e4b3ae027bc6f43a01fe471615f3a319afd9bb63f55b13e681ac0ae830d4d3057882fe247ca4decbb26af811282f59ee89ea38642e4ffad9bdfae44bcdbc3a289bf431e0bfc68148c12ced1853e698e74f74e24aa434937390fd41cb4e78f823a262900f2f44c1fa"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-224, 192, 192) #9
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"b5c4acc63ae5c68ca404bded2d36a391e8b2e9ef3b32eb598aa94fd6b5ede6c3d9c33ec77a195abb6f8cbcafb6c492a1d78f04439bdc442168d1eccc783d53a92e16b90ccbdb0284b383cb96af04e81728d1cda0":"b3e6df5e9ae10c63da4269de170550b92dde7c6e33af228e":"c9787b641b5c881dae53a69e2b3514ce2ea81e5879765bd1":"e4abedcfc4cc69da45467bf2bfb03d823abc19a746e3c582":"e14f46dcab0ba39965f170f01a07308090b051127685ada6601112aa236093f7a760530f856617d9e027c8279ef33d9fbc4b624ae26a277b9e6077ac71e2d2f101b84ebed007ddeddb4286aa4729cb3b28798387b757d8e99a7b6d2631601fe7ab4caad7983dede59b94f4c920ef1b29"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-224, 192, 192) #10
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"7302ea40e214308136b8427e601ad61132d195f870f2a861c7b8ce1f686bf325a155d0aae1211401bb844893dba2909060c76cf9cda757d9e2cb24f5602fedf6a7412f49497c82866a8c9b56e2bbaf912f760255":"58efaa77c9bf446ce8d3f3ce73b7d1f014bdeffea2a2fdde":"68f9eab1893186d7e5cf3a8c37bf1c229344

abdceecd9de5":"a0d3bf1de632fb19ca5326d936f79aafe59a0e809b13f10c":"f2c6a717ab10a9cc89f6d3a07bf6077fa3
3c2e5d67475ebcdd1b895fd0067941ed3fd8f251352403c2680df2319a882f39a91f8ccb7df2c06a13037f057962e23b8
ea0654ef9bfc19b6ec982e539ea6afcd1145cee582d27b708691354b4c397a51d004c61687c1c9c948576009002ee"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-224, 192, 192) #11
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"48ce334fcdeae603c54fc228461e7173681a8e8387e0c048c2acfdd6a78c9
55deb7dc25bea4e9924c4a2ae22d9fb6b227452addd0b6eda7769f9ceaaf2ca34568b3c198ebdcf5f6ed11f863097bd56f
42d648862":"6bf4c173d264dce03e475fb3bde9fca2474877627bfb0c5d":"2a728f461ce1067dd38896002724b4967c1
a9cfececd3437":"2b862cd7a94c1776b26022c27c0e4f2d199ccb782caae6dd":"07f80326ea781bd95efe729867d6c394
65213bb698b5e486e6c5f27d3fac4fda3cfb7c831fe6291062d4db2aff59781efb4f4cf428236aad6a55111b969885a6b8
51d5462278d0863909a07796e5e0e8448fc0d674a4408cd9e91e98e3adcec2064ad37dcc566faa80149519f5ea261c"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-224, 192, 192) #12
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"b23c748a9c9d206ed4ce6b8bacb6f7e17cacf5649ea8d1e1144a96e977a4c
b22c0f37139c3eedbcc8b9024c6f21412f1600fcde1488f95744446df7b6e21a858224b9294a75829a014697cc4b363c3
ad0e152ca6":"325bdbd8c14b766d4a7ff0e14128585b21af76de7ca30ff1":"2e002a406bb8090eae6c950944a4d6768c8
9d43cc0d8bd17":"4828622ff56d0867bbad03bac51b8c939a5dfa33a362b129":"58cebdf4676a21ded5eba4dd19452f5
dec909c589751879ea4249a4c9fef834d85dcfc95ada82f7fba1476451774036246d7a496d4d427f37647ebc10fc2e112
5b0b71da1fa5f1479c5681e9d7acc9b88b527390734d943bff6a76c4b22bb4f6ac331f7710b95f6806fa35a29a2fa35f"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-224, 192, 192) #13
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"606f388e8ae35faf979434656144370991e89b7457ca5b55d5bf2b48fe8cb
64f549f48a812edbbb4cff895efb21c90eb26c1db239ed72da43504a1e09c56fe144f2d09242f2670dbe2561456d93835
2125b19131":"5e039f38d6f9a9c4ecc67158f40d3c8de61808fd7476fbf7":"21c7d976da71bcde51a3b4bc1b9a79cc6c4
ca51ec992e479":"bac1c5904816c3040eb532622f127ac3e28cd78ba68404a9":"5f951dd774bc1a0818b249ffc51348bf
1f36aa4b9d6a3348d36df84b5d3e824adcdf8b87ffecfec13fe36ca354625ae8db8a69722254c3f6e7027b866c529f9bed
25360e0cee7ce41f996d50d224a08e965e0e5dd67a77142e2a3de0d559b9dae8919ad0387ba5fdef699e42016d7291"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-224, 192, 192) #14
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA224:"be16ca52551a6a0656c40539e3155eebbc416cbfe212101f8edc2f7118472
907ae9b2b9574abe81257533115472610ab401d1ce1f8998884af43fa5776a59ae38c88631a066fa85d24dfc9b2547caa
e598cd0fa7":"ed000ad2e479513861014e8ff45a481a494af312d2dd5563":"feb295c74975f1e1c738988fc70b9d2603c
7da93832154a1":"764705681b7781573af811fa7751dbc27d667af7a1e59dce":"ba4a0583d8d6c5b4216a0875cfad594
485858dc7f9ef265d4ed0c0f0fbfcaaf5ae318df2d7fc530301813d9f49826030625f7ea02d0630b3573c486b1fa0ef4269
cbfb6fb86675c11fb7c0570cf7ff4fc7affdb00625ac453c23c229a4ea5f540c66f031ab3462f7d12659eec990501f"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 0, 0) #0
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"9969e54b4703ff31785b879a7e5c0eae0d3e309559e9fe96b0676d49d591
ea4d07d20d46d064757d3023cac2376127abc60f2999100f738c10f74792676a3fc4a262d13721798046e29a29518156

9f54c11d4524c9071bd3096015fcf7bc24a607f22fa065c937658a2a77a8699089f4":"":"":"":"abc015856094803a938d
ffd20da94843870ef935b82cfec17706b8f551b8385044235dd44b599f94b39be78dd476e0cf11309c995a7334e0a78b3
7bc9586235086fa3b637ba91cf8fb65efa22a589c137531aa7b2d4e2607aac27292b01c698e6e01ae679eb87c01a89c74
22d4372d6d754ababb4bf896fcb1cd09d692d0283f"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-256, 0, 0) #1
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"371d2d3a50d8fef465b02d57f0f102e820c624b0e11703bb81badf8b0ca18
41594b0bd16c1fc0e5e1235dfd414081164c54ffd056c9cdf688284f615cfb4814cf28ac6dac05756e07e6bc9f56033666
ae35819ae359d53aad14adc9199ea154e45ee2b064955a8f334b9f62cea23d0b0":"":"":"":"b474ddc66e4cac2fdba195c
b9c5ee521f4a3ebc24e3722df281774b7c9acfa87bd5b85c1e4e559e2859f2382ecc3a820d76cacdf10ad559691b7059b
4e7f3d9a4453ffa241627a3a258b3439ab7f592e95751c826b6f89c92d1f85fc855d231045c405941b9a8b5101f76e6afe
d9c2032712eb5c60c16a7ecfc26ba0d47adf04"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 0, 0) #2
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"60e5cc3b260a0fdb9e994bb7c7b7fc32ef0117813a33b4f6af13ed81a61ed
c3c7209beb9336855fe207fcfb77356894b4fba0b7c3a93cf6cdfdafdb4b56cf0938f2cc18ed54a02a3551247ee10e606b
0aaa8d30cbe0bdd3781a1b238e19cbd86a2dbdcaa9f94c3d39f9deb8c4a6801e7":"":"":"":"628ad20bad88e5b0ee3010
7640248a81f7c1ef77f757a40e53927d3b10adc5b734d379d71a28b3fbc0787d6054cfa926a5a74b464b818f8d1854307
73e7ab055f9647eec01a71dcf680abf7589329e1248ad9df205d10ceccd1bdfe4c9b3f6d7b804c5114c1406db83c921c8
28df36f5755e989520274669f7f06f5550c97d4f"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 0, 0) #3
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"5b9320748b1c4c44624b26504e9e9765a136f965c5a8d787585391782c7
432e33e5d97a4c05394d570402b908f54b80cafe9be7eba6c4c4424ff53adca50b522a0ec1b51efea35bf474fc6a0d6aa6
7d44582c01f287f8a8a9caeb571e26f86100990e5633139b56f4c733cd5ad08c4df":"":"":"":"70883300ef578f796d8f8
5a30cd8b9e4e2c29f84b7b127836450571408c92b5a1b5bb040f83bced508f26d7066ee0b6e6364eeb1c639a5292050f
755fc78e828c08054b14e3a9993c2685791e2eb1dbf258cb762ecde1aa2ed41fc004ac989e0fc26e245ec87a96004c5b2
8c45d8d9e0829bdb696137f9c944f538c28be34b05"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-256, 0, 0) #4
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"35a17d1251628f82da8b4b35b979783f50e76b2cd77e03ab2f64d29d26b2
2d82a7b89cc8ba85c70e10d42adc80da014a11cbac5342d46634dcbb33baea277a67afec23b3f50875e4b965b3565de6
6e36025e0db252b1b31e45683a9676b55f462abbf6887fcd770599b123f109e5c9fd":"":"":"":"86e2bb0f5ddd9389786
92ef93d19d34865a04484cf82aaacf4546378e2198a2d8050ddf53ab618fb98f9bc59a614e3d60be06a54eccc7e3e54bce
7afaf979a6ff4d7fa19a9d7669656fa21fbefa9a70b134c01844c0b85a86b9f98a14255158ae8f5822ee506f88e81f09760
810b19f4129d6b47a10d8837d633671558ec3771"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 0, 0) #5
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"3d6c40cceeaca0633c2dc71b7135be9d64d07aa80e6f3a86f43775855f14d
3a4f5b702ec622e0c84eb3fd4662ae150ec364d343fd8068b87a8b29e9da7f181b91aa002639980da5489720068816df1

44ce1c01ea38915b6207374cae626f7199a42d47c9232094d16a04c368f0c11d30":"":"":"":"75eb7a740b6284358f1b2f7c8c1875c027eeb05e0350179f7bfdba23dc823285cbc33cfa6ca22c8e70bba00e903d3f71ca66a1d7081f742574613c2e8854a0d0e59cbac17356b1abb65b533bf563d8169700e196d7d1e25be8e4ed4502298b21dba8ef822c565443c46a8ec08bf3cbe11ac51eb765e53d2b035a8afa29ed1147"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-256, 0, 0) #6
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"6174ea125101e34850e11dcbb0e48dfed7834efd45dc9d196a42e9bbebc9f00853467570badf39ac3366084682491479ec5e80af6d5e73e0cea43d1ce15c277ccf5bee254c2d4e57623a17653d48bd82d801b0cab2df27f804e23e4dc1dae0b7eb6160264c8ca4712d775970a8756a0e":"":"":"":"a9d269c3771e1fd3cf2a5f4470c7e6560c4db008cce0f4c0d1ed939157567cbfcc2353c19e5c1b535c02d5601b45ea2a1d8045b42df6508b7389fdf350c107dae05da4e6e1c078a26aec3d0ee5225a680c15c563e3727d352bc257d3a4defda48e6dfdd5c7001439cc587ff033c5afd3b1fb7c618b2113736a362058adf12968"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 0, 0) #7
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"6a7df1ea8b6d92fb4f1b66b6014c97466a9b9edfc68de647a8a4c36dcb0f4d776bb353bbd5c18ddc5aa274ff29abecc946eeae7eb7e931673c1ba88ec99d3105059dd1f9a7ba8145e0bc86459e525028dce62564a7bbb5479320d75cafe40b4c7a0daaa2bed5a48a0eaeaaa8d6c76d1b":"":"":"":"32e66872ffbc6d93da7f923f82574e3273c81a289257246d3e69b94365115e2b91ddcb077034914f0bf3b5871b62ab773decd00121c87439ad5318adeac31ac024b46e7b49cee5fe0f1dae93a4b93d4245c016ae6a7ba7e9e9857a38b4c220c3a30903eabaa3210d93a08f703626ead078d59b28a42d76081e9b67d7ab68b366"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 0, 0) #8
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"0a9056319735191d4eab3b70f533e59b0a5a70aeeb5c00cdeaa5dd26ba7af09f2e259bd4e04cc9f5ba8b5c8dedf7b155a1ad8112d6b1daead36cdd337266fab65c85824f878219e611d48c4f73ac7c0b96e40762c87d1a78e63e3b266f5fd7b9ce86252b9bf46b0855238602c098204e":"":"":"":"0ea1662f0b95b6c1cbeb82f7b7523eba3f569544b0841f78b1c05809fdffb776eaa6d1c77a8b60ddc680c18eaf9096013d2f4bbd41617e3c482d29aca8d84822c07b55825e46a26abe7c39fe17d2228e399cb88e36e435438ca919b37a0f868fb5243afdc2cccea3b06fd313aba67dc688203878d2be0f4f8864d831622b6f4d"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-256, 0, 0) #9
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"9ee3fca776f4e7336f5336e426d8208848c854c7b0b271d6ec84dd3e86a86fab42c0825cf2be769f7e31924b34a3a760c94d0db714b2a09ccbe26b2acc8071f083332c3ef50802b2aee1eef195b74e9eba52fa49901d67585a766a9465d3db843d3f0a4a3a9d535dd976dd98aedd9df8":"":"":"":"1c1151e976bdb947bdf7bed108c742428aab2e6f5ac7cbcca6fcf2459d2410bf6ad89636b02337a453a21bf1aa72f393deadc925f9a4dc7ff978ba837c58ea30267cfe61dbca4a366b9ab9904ca6223f76d2d33d8d3deb959c6c57baba368e9e67f2d9d4d3758d072df868d2aebebedfca3bfcc018cdb19ba37b593a0ae80c6e"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 0, 0) #10
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"1006e3b161fdd1f30442346fc91b3371a29531bc9964f84d3fefd0ea3a340efc06096974bbd600cb644db66b738ffcec05696a981e50c7f6864a8279e83985ddd42a9c74affdfdc8452ac25575def3a

f3250da95f0182331dcc7d2d50ff71dcde00f92b6874ee902e613779de0789dde":"":"":"":"3bee9fe6d08899fc7eb6e1f0978c68f5dc9dcc76fbfaea7a652d0ad22632396d6e065fef14aafac7d3afb066ea743f0cfba804cc9686405ac966ba7a291f5dbd54dde5d6a330383b2355319e3ef4056b856386cf8378a5e11d9d36b0207e2cd414f9ade2af057c53c8c31e72fe765f0582da5a685eb42a0fd969dbde2642c4f5"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-256, 0, 0) #11
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"83d0546d20fe18184c5ee79bea6f5818881d158dcc7780c0350baad7662d3b0578bfe5590b9923c3500ccf96a797d9fb246f31e6b2454c6a443233ce0264fcc0ffd41f0a3bdccdd9417d1614aee596880571ea5f2e62fd6c6e555613024262a26a169f17380a19f2e5020ad3359e4842":"":"":"":"0e453a3e0a4d58f418018f09c1b7ee5e3df81d309e54b77567b180437c258b870069c0257bb8db332e9d790ed325633260967e898e7933d38832fe7a677c9484992918421c75d7072b9c04162b202872200e28db3c03d157c8adb077c4c8a661c534ff5c1bdcce80ef047eb197b0bf3939daa8be31d6156e9d573cca4b11008d"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 0, 0) #12
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"fb09b02011b54f9fa2a30783141a520e11fe3e2dd55b25799c19be9fa7bf3c20e8fbb8fe9e43014516d25c6930865c2727827cc01406aaa1827bf2d9272ebe18a44ca74d63b3b78fd67e61d5d96db509a77c857ae04e06bdcebb7aa491d1b9a99a0ecb8c7dc3d7bc69775721b75289aa":"":"":"":"ef8783f00156c497796d787c018c9c01cfef9357cff2ba8f047109a0d17f719ac46952a7147e7fe8d60fdebe2c744e50522e09aa0d18de258459840ae320d48cb71ba11432169ddcdd15ce081f3ee9719cae4ba601bda1cbbaf9ebe82559b69107111c96e468d23e0268e53c9430cebe7cb02b547d6913b76e4c1643b2a2045a"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 0, 0) #13
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"07de9e5e57368e7833177066c804575d984bbf9ca4bf03ea3118dce063027b2a1da1e930b356722ea0c0f02e09db6e92f407fd606fbddbcb3e574f0ef548c12b97460e2079a004c1b5f4612ced9f5034d8ed92d5e98eb176db2eba898915f31af7cd0763e7da1e64ba132a08deb82864":"":"":"":"e780aa6744f592da3fef690e78fe8c4fd40c364cf5f1a8be34f23f7324ab387b09aa3b5c126bbb5fb25fdd26d4e536f2eaca8f0ea8c93ac863c1c5d80314480fd9e2382ee1d9b17828b7f3716ee669b9f369655091f0ee23163996c7c815c3f5e705c9e48c25fec05a485eb39f3814065283dd1d0c37cdb7713acf24e3484afa"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-256, 0, 0) #14
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"5957069eb143c1526826c15358e0e949096108fc6e09537cf3d6426e155b4178bff8a8b7c57c3cbf8f9c78b52d76509c1ec089e083b29c0adbd7d703b3e0beeb2118a052548fb1e30455b080c111cbda6b4930e8fb7daf431060778445bad7d9c3f78dbf811e6c9c58493844d90e73c7":"":"":"":"2f5b7e172c5e291f68d9f59f0d14ec516e7e80c2eee36d1aa0734e3f819a976c74a565ad03334fbf1c60dacb1a6d150ce1316b5c256ca85c80fcee6ce0c7004a0a0ca8be5dce19a3b68f92f3f6b7f8e9c4a3177b93529b32b78a2d0ca18b27fe80b42546d1211587acee2bd5a63f3ae66b5e5d66a52154b52bea2b71cb05b9ec"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 0, 256) #0
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"2cad88b2b6a06e703de46185ccb2ddcf5e0ee030995ebdf95cc4fbc38441f17f32310770e04172c0cf91f6590cce44a4448bfbc5ce9e3b9da3e9642daecd994dfe373e75253e8eb585141224eca7ad

7bafb57f69799c0b892b3015990e133698d543aa87829ace868e4a5e9525d62357":"":"ef6da5e6530e0d621749ab192e06327e995c3ac0c3963ab8c8cd2df2839ab5df":"44278b31ed853f0a510bd14650ac4b4971d8b426799a43511d016be68dedbb8d":"4c7dfbe509dc5a3ac26998723c6a44cad20b197fc86117c778d1568ab828923862885e97198f77a1cb45113f5d78726a0f120aec94afc45f57c8dcc1cb092b343480012858ef5bc559f57023442209326ec4a54d91ca3a77dfdf9e75f117cef50e6fd2dc9af6ddce8e6515b4a97357a97b6cd274f68a042fa41bbd7b7261b034"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 0, 256) #1
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"b91fe9efdd9b7d20b6ece02fdb7624ce41c83a4a127f3e2fae0599eab506710d0c4cb40526c6bdf57f2a3df2b5497bdaef67509ca77ddfb72d8101a462816a695bb33745a7348e2646d926a219d4944397755353bab4a6b291607179d16b4a249a3466cc33ab0798517872b279fd2cff":"":"17c156cbcc50d6037d4576a37576c14a661b2edfb02e7d566d993bc658da03f6":"7c7b4a4b325e6f6734f5214cf996f9bf1c8c81d39b606a44c603a2fb132019b7":"9cdc638a192322660cc5b9d7fb2ab031e38a36a85aa814da1ea9ccfeb82644839ff6ffaac898b830353b3d36d249d440620a65107655efc0959ca7da3fcfb77bc6e12852fc0ce2370d83a7514b31473ce13cae7001c8a3d3c2ac779cd168779b58273ba50fc27a8b046562d5e8d6fe2aafd3d3febd18fbcdcd66b5016966a03c"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-256, 0, 256) #2
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"a46367f0ca034a86604003faed2ba524b6c0bba8418fb158ba13a8f730d91ec49b3a7e35c619f0e1abda6d140b08af85e3cfe402b62a2e893fe0244e88b9a489a1035d287947139af7873e5f7d0485e87238bb11d4f631090c34365222eb95baf7b865be5f6410ea0aa0484e3de55483":"":"aa020a1aa92f8a426c5d0d44191c6b46f68c1abbd5dcbcff0df2c8e024a3288c":"38965ad5f163f663b3d90d4f5b67ed2f4db22c90e5878bddcd4f230dc77f4b0a":"6c7edf375281b751383211a3e09e46c61a9c425fe326041063f0f03e1cfc01e8a830f9c4bf77377c4a9946c61a8b7cc664b22973c556437c9f5557b1a1222c45789eb700e1184d5d6e52f597ba5b1deae3dd3cb2d8325ed5b3929946e3fcf9e4f199115eafba9abc87558fcecc63723cd8cdc8dfba48a3c64e8a70995b0c7ece"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 0, 256) #3
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"08b9db82f179055872383f58203aab4b9b701c6d7a1cd428bc1860cc70e4111dd5cff962725b20d8121fb4f484a846c8fcae938683cc1602b692ad88b2edb5ec1c8dd408f4c10ee77a460bbc40c8e365d5b0bab8b6c8fb3d6ae8f65dc91750600592d1f0f9ff661d39436329263b9213":"":"88ebaa296598dd71d22ad5cdbd16603e1982d3b00391e0e83862d765148173da":"4fe9752a5a88ec1eba5e7d85b193910f1717d166ed16e12676cf9dd417d96f2b":"b4b02be55fad8dae22716f95038cce34f654c3dceac59a39ee85c55c6a10864e19dfa5710231138efdfcfa73652e99fa3febde8b06ad06af23ded42d78bd7e05ffed6b403df2320de419a08065dd254e5c676c16aec3b82774f014811cb6f32f96bb240bca91fb9f05b57c776d4474d309cb08a730c269627b63858821657e8b"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 0, 256) #4
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"76b0ba5992daab1aa40ebe377ca2e0f6407eb1729961151d216a9989b49733c2f7892eeee64338d8ff151db27b20e66684015bb1b433a01fd7570e2434bf39d924d19096199e367dcda87af7ac8b9f2a064e8a7bc291a904fc5a40cffb306020d718de11d3cdc5442724f4538d835f76":"":"f8b63da99a35cd63334c7f0f101a80b101990f7646d31eb58bd4cac251f434c2":"46a417f4938d88406d3ac65dffffff7e3c410b0999e9c6dc7787ac46a0b1be77":"d557b0064c6d8feadb23f9752cdaf5e443a295ba97e5fe3db8bdc3a502b12394951e69497638a758e7315323c4d9443ec8f144f9dff421b0feab8d541fdc3b5993dae6db4a732d573d27f4383f825783b8d0b93951719b95ddef703f36c1d95034b4c0b12615aed9314067c35a55a091fdbc3a459a22a75b6d1616e79d551b2a"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 0, 256) #5
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"e82960489c01468263e8fe59ac341af1cedc5595ef1677c00190f87f10679295b0d64271e860e5e1bc2b7c24c2127c9457ab6db2495d422d24f3560a909513626cc0e0e8d74171ca51d3d1d31777fcd1b771f5b186516d45a270a7c5c96f098c5051cd79ffb04c7981cda36a68eef347":"":"9d544530ee12e9cb06172d79ae291932e17b240f9cd92698b6a2ec061fc132cf":"dd1ad16a1f9decc0cb875ce35c7ad1a3105818679a12b22149b5a7dd0a1b7d87":"9a08d941e9a1bfd9c3e059dd06caf008c636ca08bb2e136d0bdf162c433218045224bfd8d75b8241025f93c4a8203c6ea1fce63c37bb20444c5d4a68b13ee663b262c685630d2a6c40ec224027d75bfd3dc73e1d538400789f2221ffe0ff1bff8f514c0229e684422d77b2b0298c0ba8a2ab02610e880232bf516f8ab507c461"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-256, 0, 256) #6
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"a1982c8ea6aa75e5c0486bb26ab8c9dcf3d13034372207bcf103adca982bd902b1388afd3745a00be19abbdeb12225db35ab41471d93c02aaa2414354626246b3ea3d932dd522e5ff0fa81c9bb7bb1f372d851b57043789abc1837d33d52779b638aa2bd1693caa52ec7b0824adb8470":"":"2d0113c4f225e47b5910cbda7d27d98fe2bcc23d7bc293da1028e20848804353":"f6d92fe0603e2548fc13a560f4b1009a2cf63ff91c74b17cb4f256611173ef17":"d26b469920ec26d6891d5243d3c131f129832695a130386511f02a66e92d538bd165d9bcb70ba5e8df479576b4342a27f3ce113584e0262f8eec814f0c97d48988c39ba548e4da78601103abf9c6a47ff3705fcfb7d1a150535d4af2fa219509e94bd8e74f3a90fd0ffa63159b4b62eb533193f9df3c86864f9b5f05249175a1"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 0, 256) #7
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"feecfb3ecb1b1322b34d90f25fffa2ff0c2af010a942a0467c04e9338832c3c0e5c5876ddf0e3dbdc2d63416fd77daf6170d67fd6b7ff621b1e844914711817ece93e5edf428a6e6325193d42bd676598ef4672cf1e4de4b54df68d0fa8d268868813162fa712d294491d338b65f27f8":"":"d1e3da59674d0ce33cc3e6e56292ef47fc1b3f495871f5a74a8c3f61edeb593e":"74d491697d72689a19c58982621e68a336ba9f7143c199dacc3f37508ef5f3a7":"78de8963019611fde15ee0c8c7b8a35c16a5ea1e86fdb435c422184cf0f7bbce3d6dd7aae11b6397ca213c0aca63188d3982c2451401845d02fa0822ad2f9190022f6c099d137c5a44d9d74a77c75bba2350f1269b6bf90507736d8576b53dfa14ccf7c685ea0acc8484d6a5d310b15bf3941666178414aae3d76d6d5f4aea9a"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 0, 256) #8
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"1d6bdef15811731f6e30d66c79104224c5ed9d455bf9fa2d3442e8d61395d53ca6e3d5b3862fd0d0b2ecf3577e2ddd124f7e33bf11a7ecebcd2b26a117c3805bc93b98ee0e70b8ed51b929cf76f2fa72b433757da47b1ec92c11fd91921b171ff51a41a996866e8c287ea130f06cd95f":"":"f25347f88fb41d65602b99a370be7c8ce1dd6a29a0a7401b4a3279b3e563cf4b":"4e5c80bd7ffc931fb57632935faff2f28c4f75336fd28f14f7fc27a12c7cb41b":"54a280962af1a839b470b42456a4381eb8cc26f16303bb97b6f709f91a914ed72a8b85d16ad4d26a900c8fec4148cc42f9416dd19f31fd1afd527f5fb266b6aff100f890b57c8a3f9228462d4dd92dbd5af2f9daf05e5ee2843e56f0e180eba8a2cabab36f739a7fd3c04228ec007ef43ebbc25841b7373f2c06fdfbc66f8322"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-256, 0, 256) #9
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"294c6459958425d309d4df6617410f34e96efbc1e609178f4105071171d271cbb698b79c7f83851ab0a4e29a756b058584cd5d446a25f77749e4154628c3d6963c369585a7768baeca0fe21cc40b

00a87144cbdaeba812bb1dd8a18e4d7e50e810885ac520e44c398d1b3c41fcaf6c36":"":"0e433b8a3920ebe0053e388d0f2588123c6ce644280dba77632bea8de1b6fd9d":"411a39921ad892db7d38f51c51148296cbf510a59fcf4fd2785c2acf310fae6f":"04c64a3c4ef8cd3aa322596cfe08e34b435bb55943c6ba7abf72b549d4a057e3bfeb53fa4e2adbee63c88684bbd5b84c4c1358c9c0ff0ffeb1c8fc972c4e79641c9a4ea0901d9c85fb9ac5eeb5d5dbdd324649c0db542e0946d96cec8a990147be80f46685cf8278b8cf89c9255baa566740c4fd12e6bc163be6e52ab7799c2a"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 0, 256) #10
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"1940c31637da2a1a4a3ad66826e074a0d5ce69dde50b75a55b5e09daf23c097bb31a4e9d363f3c716cd9e899cd98bbdaf67e6f909077c7051b067d9f2a6ecace36e5053b2e6329ffd364e589403a0be1af2b27d258c90e1cb2d8261bcc7bd5f910f15851a87442cafe87aa42031befd5":"":"0e21b2eae0d946c1da14153d9a3945894f43ae5331ab95a07a727b05bffe9f35":"69646ac749185da00638654c813d45e0dcc842202845cbb0a8158b2609733146":"f5dc9a88bcb19f74101fb46304bfd66fe0e245357b656e751a9ed535bed3a5b47f4f84c01068763a3fead22c29d7def5d18e32453f806424177082d1d65dbe3ee5d9765fd5364a1cf55dc64ee9f3f313697c2625327373298807a60bb4536c3040e76c9995cfc6eef225a122c98849980d40ea0f86a122756d4390096b4d8fac"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 0, 256) #11
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"83a44c38f699a883a91ecbbd9db952a62b65cbf75e72a1a2497810a73ea743c4d15ffcba06cd7a3338b3294afb50462b1eb4df21dbe7107a8b4c6a41b41977f38c33b1ada829517d0902a3bc0836bf899c257234f7f63219acdcdcdfa510d284e7380348296eaab4074ccfa9037e6b68":"":"3f6f8f77f3051c945afad9969af764fcf4ba5b567c0a096bec36f712f0405539":"210ab7859b1354f53e143e8b06afe84b12fc1b16aa4e3e818dc56292656eb3f3":"adc004394a5bf98be1ac40123ab1e430bf93046df87d20b04c235d16543c9a2b80f99f841a946e91a4c6f10149f7a703967de651e3af208d600ebc2c6e2c1fbc895760de537a4da2870e128fb10d8fa1f06870d758b9804c49c2ab81f90118042f78a89809b92c2abce87b230587739acbffd082aaba422c88e7ce199691dd87"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 0, 256) #12
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"7a45d07a2bec078c06031b79e94ba6b34ea1522504f62df3c7543d6a902a352faea5251586a8bdc562aebfd9f7175a025406525dab022350d8452cf3e187e30cb54320fe9f13a351e003727278fdd12c2ac1bf56556317ad5bffb3c2f89069c7c742be442f64972304a3a97ad40481cb":"":"16384f8c9eb749fb49fed4a667339f2284634a5f791369739d0401a84d435373":"1b81f0d21a3da462ec2f81d0bfda1fc0143673b80bc7ecdbe524ceba9ae96ddf":"a34623e01a14b87c400f681a6fb4ae66b97afbfe040758b99dc807fbac73d22a5cadad262f23ea5d27f726993c8220921125cc78d17a990145bf6845c7719bcbdd195348c40da96fcd60a54cee25af89c3b1312d88635223ea8c27564e918289fd0120b437c42d99a35f198de3e9c092c493a971c8ace8c48ab625a5a92d6fd0"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-256, 0, 256) #13
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"646d1c1e7c363c4cbae7e6a4f606c95812a7e0f2fb86e33f178f5b502c6457d3b57644b3bc1ab6ceb09589870c7d54ca19fe763b481308a64667913cfe25103fe738fc0a800920f0afec70ef86cb8a0ea2d9dfd3895cbf921c87e64905f81ef61dc231b6cd7a0135003726451cab95f2":"":"78566b2ffd3252772e3bba71f3445497a2150afd48bc130251baeb4332da8a27":"888b33c6abdcd475586e00eef185a69726eb9b024be447e9298b953fd8021906":"e659d60d17da14043cb919709bbb5b3cc5a203517353c8badc0634ef2f2ea2dab6fb2b327e296ed6341dc4bf431c0c14ec041de50395d25a4a4cd64a6420153a50af886f48a2973523a4ec5baff43526556959a37f3b2452d5753f4d2a3c050b2e8f9f6ac2577959f346ab37404d029ca51a789a5521ee660845f913d2452033"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 0, 256) #14
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"bde2de2b8d3c4b5c4af2998d70da9a21340b98c7630d687d685a71eafcce
c446e0194d245d2811a54ef522dcfd96abca2ecea6d7892dddaa4dcacf7e5ef3fb345c33b23a3de687ab578aac8e675754
7a1b3c127a633e58903e8367a805840020d2ce3f6f0372991d7c7f234c3b31118b":"":"d903a2271f1ce24f20222120f8f
ee3b8709ce4fc7ba85b77d6ff049e81d7a37f":"03bffe38ef883397cfe53edf6c79e68493b7a637d1ceeed9d569ac6195b
8e4db":"cc317f81c3a6cab42933d1733cfc4504dc0b232dc00502d29b8e6fe78ae11d1d1ae4a1c5c6a7f99543a844ec54
13b6dc3c22e3bf0cbf12e7b57a48018c75f6ab25fe78b786d2d035de7adaa3a3b7cf1ca564f342fff4f9e6b3c9d2af384cb
70f5abcd28c99a5d10f176dd2f702575bfb81a984db2507434b4a3c8c286e3dfc68"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 256, 0) #0
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"f7b90c797a4a376cdd9f5c435f5985e77f36ec1df1145a12072cbb2a0da37
8fcd95202986d45896e9f4a65f2f353fa35130ab64f41a5d49d6a241e0260b4bb8a46a16c6ac9e234c84b5b26cdb518d4
59f7670e817ac061ac60439be60982492000dc5da8bc6636bdac8b1cab03198dfd":"61535c5c045e784267fd0d85f286
1778fa53c8e8586af67cf5c9f21a28ebb656":"":"":"8df4e349f9ea43cc509ecb2b1124358cda2de1f5cc9315edca63610a
413478d68b8bb49c2814c82ce571f6e0a6780fa21c4b570610ee0c04d3edb92124f580f962d741330200c19885ca7165
02223247b728d66fbbeb7c6cc25cfe9866b1450b346227c7663074c8b15d189f1c6edba172a53c733d67c1c69bd7aca7
e62013cd"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 256, 0) #1
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"135496fc1b7d28f318c9a789b6b3c872ac00d459362505afa5db96cb3c58
4687a5aabf203bfe230ed1c7410f3fc9b367e2bdb7480806f3e1933cac79a72b11dae32ee191a50219572028adf260d7c
d458bd469fcff599595c651de71685ffcf94aabec5acbbed3661ffa74d3aca67460":"64b6fc60bc6176236d3f4a0fe1b4d5
209e70dd03536dbfcecd5680bcb815c8aa":"":"":"1f9eafe4d246b747414c659901e93bbb830c0ab0c13ae2b3314eeb93
73ee0b26c263a5754599d45c9fa1d445876b206140ea78a532df9e6617afb1889e2e23ddc1da139788a5b65e90144eef1
3ab5cd92c979e7cd7f8ceea81f5cd71154944ce83b605fb7d30b5572c314ffcfe80b6c0130c5b9b2e8f3dfcc2a30c111b8
05ff3"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-256, 256, 0) #2
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"d78eab5329fe38a26ce2e54efcf8f0c15cd7462a5878537a1e3615d098b18
6974f48003172c7204fe6dd77c89fa92fbad4e81412c8d167bde3857b9e045bcb5c666d64aa990a7d92e46ca533b93de
544238b79b6a9551ea7dc52bfa1557fd973bf6e594ad4bc0e63b651d5955da37f6a":"e934bec18cf8e9b9293029d9ed6
0ecde1d46621439c322203f7c22c6b2d77544":"":"":"285df697361c284753c94865081c3c25ffcbc77709fc51f37a096
24bba67149156a087efa92ae709eff1bd50bed464f4f31c4b66c1cdb71a506779b50645c165a099718d599fc9a166f345
abaf8b0b2f9e700c253a454cea49262a334d79a01c208caad5073644b257b2b1577dd973862c6fc7fcc3320e24e1e3106
3fe6e94ba"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 256, 0) #3
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"fad6a0fcddeefb263c27432ecc6470e44f26aeff2840e8db682ca14ab45c31

cc89402a698ffd36ca8ffce986568f728afc08bc0077c95ce4cf08bccf50cdafc19004abc3c5ced1cc3e7ce2cfc938c1600a93fd50fef1245e7b9cae2834e7104335f8aeac080d4a4fd3e0c0ef0d67b690":"352270c867c34b3fb297cb2e5d3a807b087c720026576aa44fad577ec82015a9":"":"":"3622977f8aa0a0ca5f8e1235d03b76f92b2f26eb172b88323558e8f3c756c539ce1061de127247ca7553402c3d5c9439b4c9afbb4c419867baee06eafd856af9847a69247ddf6640a09a360c93577bfc353cdec7312e549bc7873f77796e062ad058ec7f3e52dd1ddafb4bb1186b05b5360200e6ea784be27b8f205de80ba145"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 256, 0) #4
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"be90a07ae616574d36f8366d39d6bf1408626466d40982d97380e44331f9e1885a27cab08c6a8595894de22a909dc2479cf15973a0f0b71c0ba911951f9b444050825a976c391e621c58fd4b59a7a22a7dd66d8f59a60c0010fa8aaacce99bc2aa1f365653dc0cd57b489edc2349177b":"99b88ac1958d5d62aa39eca8b8f8e598a55c08b49e895737d74b8792ca343a36":"":"":"ee76c5a6b6b4eaf9ce8dc4ac0ee91cad143f0369a2bfdf40b70fcf14e3eb28855e3c59a01ddee684bf9ce4152be5c70d290b8b780784eadb44854b03cd0a32d0aa8b8f0db1bd47502d2aa61a54e3de7fd7bdb5c74c715ae2aadfe328b4d1128bb19ce7d8166c4c1719c98b6bfeb1ce313054d8f1b6a4c5af842cf3cbea17c710"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-256, 256, 0) #5
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"31c7b8f0aafa70b4b670f056e24bf141f0bd6683453d17e9b09add3d231cee1cafe818dfd7d7343f8eb1b4100d80c4d9c8e7e4d5afcd3ab82964f121847d4466471df38b849c59630900171580948f53c41425045dc4db04935aa5264891af031b08cd48670b2b1720692cc6bed3e7b1":"769f2b3e30408856f46fc3a3fcfe05295d876415555906ecf853d59badd48eef":"":"":"9b3dc767e1bd9dd67003ec99c334b94dd97c48cccbdbfb2eed4dd5bde96b1e0ea4c24cb0edadcc5386f7bec54ac5ef149374f6225aa7e78466c34b1ea0b286499e4e2a294381e6e065abeab67553c4a2cd0fbda19c59415fee5cc1249692768aebc80ec35c8331f68f1b7245602b3ebff1eaca2fed5898213fbec09acdb60cd1"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 256, 0) #6
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"3848bad2b0631411f9168bf818a2c3cac10b6d83a82d58011367688c8d30d3fa77fe460dd459c7da7d69a3ba5576b2bc8dc15a0de18f52f79b9120b03a5bd9bb4b45547b94b301cf3ce2442ae5083c5c08b455e06fc3f80be972e2868ea019376fdf0472147828944049174 4df5cc1f0":"e5a3ebc7d533c214f4cd66d37f1dd4ff718891daef55959915938a177dd97088":"":"":"959bf36092622923e96ef5c038ca318048f9447003626a9f5f0c5082f65daf5c5ebdc7328e090fd68ee5d3c161506b86590e2229a479de7bbc3920852647db2a35272c305e9a309c04da1b8e58ee185183681cca89f1b9534c0e15c188f69cbed87326a83caffcabb800e2672691b7642700659ebccff375f284eae1729edcc9"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 256, 0) #7
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"dcd74d5dda3adffcbb54be0e7c48682174b1b460622b52ad4f32bdb2b164032bc32776da1ad3913626d9e61f5b9f9877c8bdbc62d984753560f2c292ec0ece8cf0e369b64e14ecb910997b7fd81a8eec62e9ef78b1d0de6642d8404cc4cb7bd544fc5a3b3588a16c4e342dc5003d6608":"e7aa07cf4a3f90167b486c1c4ffdd5ae45aa59200e4a94caded0b85aaae8fef2":"":"":"f931b0dae43703f7ec20bb6c5667191380e7e263efbf30bf4bd4cf6e3cd5976095eb48ddcfe9f72c299dc05ab2d8846e2259600fe3723744f4ee19c75835c07bfb207e70ceaafa355bb6c6b0a4236d0e0830759cc6673af2b4dee9a3efe496e7020556b4f8ed0c08cbd4cac61831bab2f5a81a8121b240a9c6d374172e

5a87e1"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-256, 256, 0) #8
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"b72d5604401b15477b659a373caae53a8fe983e2199187546756e039e72e
fb7f2ad472ee90447f616b7ad5bb1dc692fd1b9e1000ee6c8ba65f39a837f27a4e5cde8cbdea58ecf1145d53c219369fa8
6402ac05e3fe3d52fd54343179f237ae2055277d76d9276bbf83f97901232ba6c4":"c9038b0d468153e8529089c3db41
8fbbe42afae5613a8eea7c8e3c2a307c4159":"":"":"9c2a9dc2504e2d943d85e1c068f7e578350dfed661cb5d82cd26ce2
2d083f6e158a39161f303370ee844b4f75723ffb45131223bee8efc32726bbdbb9ba2a0d8177e90e4e1c8f1d3a22e9a9ea
ef8b7ca4cbaf142aa1da1886d2ef9c1dc3692bb15784cfc906e12b484609403515550cc44e3b0edd42ae9c3f267ae9dd7
37ef28"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 256, 0) #9
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"c5f5e519283f7d3216f2ed7765ae2c0dd1e22596d7762c1f0707ac99ad3f6
ba6b920e6d0ec15852186b77c3e9318904b252aa0e2dafc2901a5177449032a7727e523d33d6f4b5f350545e5bf21a2a
b6cea23f43c73c2cc0982541c298e05e4b2dcc6fc5d1d507232d735b01ed2536317":"9835ac84c8f8cc00464ce758910
74e20f050b162f73c9e91435aad5929b473c0":"":"":"85a747731638e09ec0254e7aa38e08439457e6504de94d00405d
417326f3ad47f156b5e211204a83634369beffc128f3614e89e2e288d2de11f7b90bcc2b8d29f149e13a3cbc8d711d247
65f480bd6596c8ef605cd72fa64ed8ab1f9a18b2d0b81c0de08a167d537b3d1c51c2a0c9ea9124c6e41613b383f13f1d2
0e1eaf2288"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 256, 0) #10
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"fb912fcad27bbb2538164f75a79a3d7651c42aba547dad64037b492a87e3
01809e154f0b8b099a2f584643e4e40ab34fa1466679fd0a8a1f82772ae0c8e9de2a461d820cf37b2e9bd77a609dc367b
449ebaecfd0aff59cabaf224d5610069c888762f92a16553d82c917553a9e723177":"e3c8eab35fbf90cad2a69cc74a68a
c0bd0fc51585231fb9c3eecb49a064043bc":"":"":"09b4a47519d4acfda506d64c0b5536fb9e72cb1b6b408da82b4b80f
f794f45beb2070b05de67759b8317f40e798bf37d392cb59cbbfecc3056259c9426415df526bf3cb62f46365426895376
29c0e91a9bec2a600ede3dcae82079ceaa3522524fc002e82c280724c4179e00dfdd374effa05a71fc856ceb21542be0bd
b62bf7"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-256, 256, 0) #11
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"ead7fa32dafaec063474693e98230bfdd61ed5ee88c7a93718fdf17db7716
73f2c3d12d63a08b9acc2ef21531412dcdac37c5828d4ab26c1e365c043aad21c52ef9c144305e917dee8a15dd6cd751c
2c45a2d6e146935458fd2ceba68b49b74bceca4329ac5d30c7a67f614d3b93a6fd":"fd3da5bb01ea75d7e32c023eec230
f3bacbc163768c1c24216028e82660e1bf2":"":"":"8fc78a425f9e846ec2c757e98f0e1f67085bde0184f9ba9e8697811f
6c50928de7ec9767a4fbec8bb099f534cabae4bcde69f2632fe4d1c582cb918e3370cabb2153a1d168fce23fafde95660e
6987d2e8fcefbdfeb21398a5074ee76f7315cd7c517d3a4df8af26f1857b0d3e5704b7a3e5c15adc5f3c6745c063d45a2b
f1ef"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 256, 0) #12
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"5d79c6ccee050b3c2ed52edcc16fc26ea7b6f3fd2b9199fd65c7dc2345d65

66e9a0c6e01710e4c71b2820f7aa9203da23515eab85a5812c66756634804e3f5817d32f51dab3ae00443c694c59b72d526f840a166e566b7f633c7d246192ef82419e3cd733a02684d6a4ca091178ccc76":"ee4c3cfa5c79b1ff1dec4b9f9ff4ea45c916e46889130cffd7f137e6579af52d":"":"":"4f53f72462d7e9247e7ad113827d3ea741c35690fa0be027b86660e937c119e7237bbc674e826f42dd6dfa5f54d90542ed2bad21683af4b1f8741ecb75b464345111cc3d383c8b7d088718a353c2d4af93ff59057745a808203d08eba2452a1a9ade75cadd0f49fcd27ac3c024c04c0936c0237fc29dcd061b62fbb73adaa8ea"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 256, 0) #13
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"35f9c3b0e5947a74d90609e6ab660b4b46177a12886cc77a19aa9eaee86500a9eaec5de5672c5ee56771d778f5aa963713ffd39fae8e05ec90843505d5832ec8d999f271812d41db4f223a5d8467944f08083a81c29d9a559a960f8349fb0174a8dbcfa171be39a8c36bcb7743c5c5b9":"b4b5fafff369997074a82e064298859ad2775eb5c5979f81d2118da96e840930":"":"":"87afd3147e61c49d2029b88482eacdace56f27ccda2927799a7dd01ff63d6873804e7b5635645ff3f65b00e1bd65254933e7e57b56177db81548fbac37305d3dcb70a5f76a222999d6ba9c73670ae931b49ccc97b4f25203ee95cd68fa79e2824e2ead8bd4755a5bb4658e02788b9ced166ea9ec5373954ad8da88791e8f1047"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-256, 256, 0) #14
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"cd08363e60e17bbc12d57954ef92ea38af1095ffec417a7f305b7c10d44f1e6500649786d5141793f7ee33a913b08f60457cdf6316357035abf57c2e2b19bae6973d01e9e93dac249198188be2f6849e5a9636d6b6bf7d1c01c16c03669ab7b5aea828017989c870cac6857bf327b748":"b5611807d3070200fc6257cc2b13a84f842ad45ce116fc91eda79ff14f3f25f3":"":"":"281e9ceb5a46578dfa2917d9883f1819bbbdc9901d44f3ab48ccfcb807eb596e20fc05060d6a77d92a6f630bd2a012b41232dce411ea046794ab0096b86491d3ca2a59d4405e2831b1f9f69e55542aec89417ee7ecd7a050eb28fd4d7d2739aef7aa6f30fa17c5b2bc1c69ebb10163426b8c6033ec7733cc9ffcae2f23986e63"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 256, 256) #0
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"4294671d493dc085b5184607d7de2ff2b6aceb734a1b026f6cfee7c5a90f03dad071544e599235d5eb38b64b551d2a6edb9b4790b62336fbb9a684b82947065393eeef8f57bd2477141ad17e776dac344a9abe80f6f522f29878bedf8245b27940a76471006fb4a4110beb4decb6c341":"63bc769ae1d95a98bde870e4db7776297041d37c8a5c688d4e024b78d83f4d78":"28848becd3f47696f124f4b14853a456156f69be583a7d4682cff8d44b39e1d3":"8bfce0b7132661c3cd78175d83926f643e36f7608eec2c5dac3ddcbacc8c2182":"e580dc969194b2b18a97478aef9d1a72390aff14562747bf080d741527a6655ce7fc135325b457483a9f9c70f91165a811cf4524b50d51199a0df3bd60d12abac27d0bf6618e6b114e05420352e23f3603dfe8a225dc19b3d1fff1dc245dc6b1df24c741744bec3f9437dbbf222df84881a457a589e7815ef132f686b760f012"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 256, 256) #1
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"c7ccbc677e21661e272b63dd3a78dcdf666d3f24aecf3701a90d898aa7dc8158aeb210157e18446d13eadf3785fe81fb7ba1915b3c04c41b1d192f1a1881603c6c6291b7e9f5cb96bb816accb5ae55b6992cc7787e3b8812efbed3d27d2aa586da8d58734a0ab22ebb4c7ee39ab681c1":"bc55ab3cf652b0113d7b90b824c9264e5a1e770d3d584adad181e9f8eb308f6f":"18e817ffef39c7415c730303f63de85fc8abe4ab0fade8d686885528c169dd76":"ac07fcbe870ed3ea1f7eb8e79dece8e7bcf3182577354aaa00992add0a005082":"956f95fc3bb7fe3ed04e1a146c

347f7b1d0d635e489c69e64607d287f386523d98275ed754e775504ffb4dfdac2f4b77cf9e8ecc16a224cd53de3ec5555
dd5263f89dfca8b4e1eb68878635ca263984e6f2559b15f2b23b04ba5185dc2157440594cb41ecf9a36fd43e203b85991
30892ac85a43237c7372da3fad2bba006bd1"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 256, 256) #2
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"20f69bc4a308d1fa40146bfb8a3171e81a66ebf4c83fd46b2c8a3b34df499
a6c92f4bc9699bf6d19d5c3f45245bb0fb08310eb7a9ce51883b0c36271b5ff0a1c00219a04a6b571362c7a18cabc48f2f
ab0cdf3434c9f72cf5ef6a61feeedc94c72e28fb5a99345dbc7939a3b8e277c5e":"882bf0edbb66ebb288ce741997ffcd3
380049f5007b30e740ece190a01612dea":"ca1da31810bfa6c02b5863f87d39668d796105430c445db157c41a0152a0d
200":"c344b0bfe801da37e2320d36b9e6452235e6f6f4cf3190d414e859f4ee90e5de":"8ecac7a65cbfb7a849604505d4
03acaec41c6ffda3009f6080bda79e26d1de3bdfd88fc9bb9ca1dd1cd8d49e3d0cfb0f0a2e70ae1834e8f7d7f79382591e8
bea0a0386ad40c98d097122dde0dc2f4fd3258d40dcdd804fdcb72d62ef9041518c34fd8a37684bcabe2f59594382767c
2633bf255121ac735852fecf14440cb623"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-256, 256, 256) #3
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"0a13da2edd9ed097631860dc29cb2d7eff3519910808e7eb0c6ff1485cdf7
58d9793ca69779117a63a47e386433f18b882ea8c8d3179dcc1b263fb263bdbf2ab818775a881964a5690a6e9af592db
594a39a960e343bd4edb7747d75866e1ca7125797d2bf6a644aed6e3c8443f94274":"48445b1b6807b261d10569ab4b
5d8ab5d97ebd3d9e8194088b10463abf11a2df":"6b742d07c45a031795a7771eace89fab782eff6a74555fc2eabba00d1
d7b7c15":"cd0493aa84c941c1b7fce37d2e38c199fb8c86ea0c5b6a536118ae423ca7ab50":"fa005c9119a898f2fea35b
805a2bd8be88c48cbdaa8582337f1f407ce3e49dee8011bb1e4ae33317ca6d5cb645687a62aed86d5803583a012d96b8
2e7bbfbebf59fdfc1db0a92586a843f6e57056f49726e89bf98b641ea60a3c91815edbaf415b2c4eb7bb8c56ca5d84a358
7c64a945a6e3d625b6763084c2a0917de6bd6746"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 256, 256) #4
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"fffcaaa7ae7787e12e96521a3e29a7c40ae08a7cdea9974cfcb894352955e6
5a27c8b01490c9fa7593734ec27ae242a20d0371c3c664bdec7f368bf53a930cfb0933de5d50865cd757b63fa35034137
5f132dd2bf9bf8c6d9d2ca5354e284bbac677c269298e1a5bef536091081446bb":"5b1c1a19b28b09d08bf9cde87b4a6
881d38a7961bd7ba6888de06d0c78fbef13":"5ebc76ae5779fe563362c6f99bba35b4b50eacaf7192c68b82a376fb7f2b
61de":"95831949170105e9c022a7711803f9f7d617a8a137145b4c2f6ddda7ebcf3c5a":"633cb6696b97f2d4119fe242
486e8affdf1b3e25a94e434592caf0270563b210df6a9f9405c2c33cbbb750c0218f718116b67232db874621832ba78b0
40523b2ebf715082fd23fe7e32599402af95156ebeda98eff2a8f2a4e295b9afb7fadce956cabfc1183f20e4e059d91604f
a5d77065c4a006b3fb2c15750206ec936e97"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 256, 256) #5
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"ae8a6a25b266051cd41fd5ecc682b844aa3a09327216eb6ac63390250620
113124145033b99896c21f8dcf60271ba681156406ff2691886972f53c2e4b449dc94fb09a2960a3423d2f4ac66f973b4
a89f80c00af6fbe4b0bbd430b12a714d40e172e99f909916a27221020fc72259cb1":"0acbae3c085d2e5e760b0631c6ad
97d935e96b0a90ed4a9867f626951596ded2":"2d74d07e82a033c0bf65643a6478856c92f33ee55a2682c17e7c42857e
8e6fa7":"a1b397cd826af3fb1b949453e96878e59f0697352929b15cd678142453479e55":"c309567edb3d40fd8d8285
51117964e20041b031e8eb41a8c6e95e25e0f43372585854202c5d5796ca4fd38b7b789b44410ba3e3ab7016cb67936

25be27c6c8d39499c402e4d52bf2c0bce21a5f4f16d80d5449d5222aea19b64de25f8f5eb81bea7c491a329ca079a99c9ea00cbf3354b5fef435e8d4cbcbfea7486d379a2a2"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 256, 256) #6
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"e603b02ccd1b3e2cf27a2a5cbbb6e8fd205ed3531ab08ce912f915328ea1c73ba7a075a9dfd9805101ba2f0f6e42ebff7202687e99e1cc914036146e187c16b83999df442f0ff87b9d82fc7831714d820c247f1a2c3eca9d32ef0039c4a2ebb9962d844e0032a58c604d630f12884742":"27e863c2f9f91e9540f0201dba0fc63c3c623ac89d63368093dec2f17b6868bc":"93e967f73929f2be339448735c74b571a8b80c10bda2ea7fbea824b188a7db93":"1ff3a43966a8f64c42dee8889ce2626bb370afef4c0222b926abe1be719427fc":"7ca6867ef568c8c323d216db96b642576de1f5e82d08b84e6a2752000c5175cf49d6096dff7b714a45a72a69e467ee378f4eabb142eddca926a3d01120960cd7aaef1e377f447b0bcf8ee733d961d0c36be901c7f406a1dc81cb2ae2e9f6886f5ba1e481e7c1396d2c89aa456b2fb34f02a91d0eda8784c26ad5a6892ba5ffa3"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 256, 256) #7
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"222dcb4b31c7bc37d8813be78d95e9d8c0f021363862c6bee5b01e6c9dbdba8c2ae81c52b90d4cfeb80697fcf05caa08bf81702a92a6bc90b531b363db5a5fe4f50412621ba390c1cd211a9683c47ec7ed6d15513bd49d10449f0c450183f5a7b16466a37df5fc79a4ddd3ec6bd0c56f":"bcc19eb476ac96567da10da8fb714c2f9fbdff28b7c74a5cbac80ca480e61de6":"46fe8bd4c4789c373707050d0e700e50d692ba10ff2fcba20045c9efff7373f5":"68c956a95f6a2c9cdd06e461805d5270b0df3c9fcdebbeffb30dad1a852fb35a":"8a54fa9818602032762a45c9f67f668860ed605e371a6382082509249330fc24d13c4acf27782a7d2be42721bbb9c80c6338acb57a715ed17c008928166f9a090331db4fe62a11ab47c966bc3c24a8be942e350a2dee7c7e9f620386d89a1e0bd5298d00f94f9a931e50834a2a85c0175308bc74a34ac37ab21305c511866263"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-256, 256, 256) #8
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"787c1fe1498bacca291f020f80d6b556e4f0d4fa5adcf21531c447f28e14266e4f2e9de3e12557756348d8b0c73a1301f43ce41038cbb7dac60d8269495b62ca7452a9c4edcb54e7d477f0c6c6b7af61b3a3784c775a5884cc536f60132e66386dbb911577aef75fc0a68508432e255a":"91f18dd75859c2938edb0d81f9d6095a2bc7565b67403a8777cd059f2631c958":"92d2d8091cc4fe9f5cdf2ded2e358fa05a7d8e4525333b4c00697ab18dd1f995":"2263cbb6e29bb9bdbd803c7224aa039077ba43d1643d4754745f89d8bb6f888d":"620851d2a4c8b6558e18aa5e2d454cec83856d25e619e69928b578ea4d4e41c662a4cd0ae64ee756b184742154d9e7a6283d78bb8b6ce53e2fd2ce93cc12ad78749cab530a7f996c83117df6d217170927d75a0c983194816d2e21f928407912927101 78b3f7d9fe1003041d2d9e7c59943b14409abd7956bd5c31190a54ba0b"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 256, 256) #9
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"1537f9380d97e98f6e02f4b10182b835f224cca2278f37a8cb1411a1c6cb89eabcf37a8b159cdee3a55329b3816f8c656c7f63835f860b4a5e3c450a2afb5b892b4da708d39614921a82d36cf23518618c9bb0f5332492c1740fb385e969d77d5d7e0aa0a4066cb6bbba4e4c7fa8ae73":"6d89190aebd160b155d5dff8cc4393f095988a1551bb154fae621739a4378430":"04a511f1d8e1994879e2372163b5a45289966df680350bbaf9baea52333e652b":"dfd8c8e467628de6c121c403816a65bdca01dcedd05778b925283f92d3cb5251":"61edfb457546493a43fe1391b8f86da01c1242b3297f3c4ee02e04e37161725f4182b144609335f0183b477744ce3370ff64ae861c728e7526148eac3fb07403a27c3f82fba5ce505233a4e38b8d40c3f44cfe3cc65c6a89127f803b11a3f24397a20409b594e193e44319015

5da50ff1134c8b1adc5006c7ad201887e6c1ad3"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 256, 256) #10
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"842daa3d64b3c25210cb0ecbb251333c2ee4e090a992138a5d6f9c455a8a5f0d28be9fb51ad223ed196d5c245eeea940f822952bbcf1e2ba7d3dbf526ae44ad7e60e9d99a833b3f372f77adc440850f3fdeecf48941dbcecf6f710d99ae54939f9bf35c3ef2b7b6136d7778b95846af5":"bb9376b79ce2cede150036c0626ddaf8bbd960ec04ade2694be6aea6ce8946e3":"41431b7537968a2ffedd6d7942ee21565f34a5155de6e096646fc7d41302ed96":"946b190e855aa2d4fa7544e9858ec70ca9ac19ad510bd7d625f14d16a80896bb":"b0d45631a104c246a1af31c8bcf7f7bea92cde3c259fc029072c51e662a33c040cfb1d262c705320b7020bd1365288c1ba9b3bde9d0a9df8b9e7275e8637ce9a1896877e34323abe8ca3dd0262d3d75ee3a5af505235e354aab491dcfce11287b7c73dfc4c97c47f0373cb93baaf3def2186a53095fe8b050c94b1cef109c07c"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 256, 256) #11
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"aaba29c12aaa011619c07efca75a186714d97eac18d75fdc8b5b36a9ef247bef0f152b758cdbd69256bd8697fce53d2b59ae1210a350319834d6721e9da6b2cc1c0e559a26804d47953e0bd5df66ea2a0c449fc0a8dcc16b9b0a82f5e6f85a218cdddaef40c254c1030a9bfa33214ae8":"02470d6898bcd119cab49242c95fa97b56a495f6d1c5b26d1e877b70b954e3b3":"e4e4293148c31ca6bbd73706e2dd2f36a22d3af3f862ddae40ad35d51dd6781e":"34c6505eebf018676a039f201507fa38338594cd015fb4d962d1577befc63ec6":"e1556a8bca38d5c2087b5c61156ab91566a5da784647e220bf4ea0374e187d4a4bc373ec891472daa31aa0dccdb56a8b42fb2805e74251976ffe5e02b446af8ac6a9f0d6f36d857fe6d3772d9fae7ab08b360e8de2529dec80dd31a5a5468034aa53b10b6a73068fd9e046b70e2f03fded8bd85f7df4322d4fa5338c9cde0471"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 256, 256) #12
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"742fbf9f39f9d8c4279143f88a6d30307492681ccd58e8422277259a0bf87aca24c5d6dc4f650f39c3403fe1eac1ecb079e7b9f363eb44559177701f93da93aa30dc5f4b933209073c825ab2b39b52ec23caf049f760aa385f58983d9af300ec5f831f2449d2508bb5824abb622e00dd":"c2c42e63d43a765c2a49d2b35c8ba98a7a67765a0c453d2352d9f224aeb06176":"794083185e79cf918faa846bd12287e8ff1e620770e0e08b33e8e1da8d23cfda":"ed7b902eb55b7bdb2b8bf70711c1f7a4bc00c4dade92c9d2459db060551336af":"c83af90a8c7879e98b255e9c6b1852bd759ccf8f9c5be4ea5e9a356df4c43efca41303d5a322a7e42ed12b8b0b715e1d23257aaa366bb261e39f19834c38a7a883bf2f01c47a782edb7905cc61742b8166974f5990330a08168e25d4aab6740b96493ff87a424ac6ed447ad655afcfde1d2ec6ab2ba811351385ea0f8b66e318"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-256, 256, 256) #13
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"1437958fbc93c701cdd09fe81a90af55f022195388264ef03758fc08bfd0dd80f63c7bc06945eedd58893df2b5f5f62b222ee423dbcc5491d1a57155891406c79e8ef51fe7575db8074c4e40f50024daf177548eb130a8c248c2b7df99b6626ee062cd5e82048019b32cd6c7319eecdd":"c443f891534c30d8d2b1e2072cb5b824e6d3ddfdd1e6c7757e54372d4420b5ed":"39f7abd306f127baaf8cb832b67c2564287efa433df8ecabc40b9744637e6bfa":"eda6950002c866c61d2e2dfcd9d69e8c5154b45f762efd688e26044adc3957c2":"8fb758b498feb1c0e961a8f86b821bddde387dac221a8191f71b6a64caa2bcc4a475460823996f8261b8e22125dfeac5c9dbda25525dab249cbe469c5e224478964793bf822446721bf5bc85e5da6ef34ddcb7c94f109193c475904099b06e2a7f53ba6dd94480dd5bc9fff90150286c4d3ccea975925cc8ed4ef9830389b9bc"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-256, 256, 256) #14
depends_on:MBEDTLS_SHA256_C
hmac_drbg_pr:MBEDTLS_MD_SHA256:"ef9292f4a7a67ac4d4eba48936391bb45f8810c2ab02ba424cc8e4add53d1c514611e3233cd8cc8f6d69494dc336cbe1cbc67c17520af442933a235c6aa6b8f98128c66fcdd77843ae32e06b7a31689c9a6a3c540a19081bcbe850278d50adfac3638ec8cf85148a0547d28d0a7025db":"f4a8721a2a873f8fe94e4b3e137e866c79212f9c14f89be156c47a5fbb9aaecb":"b38a6628647a02c0de5b7acb939d0d1896c9c730106c8667d810bd4866ebaee4":"366370899b2a0d6f049e7d820061599a675cba5d3bc82ad747fa731bead8efb3":"1947d468ae4fa4da7f45cfaf32d62a4369796e532f1b03b1495587e6bb95d8330f5b7c962a9b0a2b715d9def79194741870e5c47d15a7308843e10616b891fc9e5cab7db901e0f1efbe1217dd627c71b54c98cec0fe1b25a84caa56f0bde247a9d9183587742a38825234b6b6cc808afde36ef5e17bcdb2c72c7645949289369"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 0, 0) #0
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"51ec4987ddacbcf6348e4a891fa571c6e3aec02879eb0181a121a4846344a687cdff97987618753202 56e5a59bc94663faab8864cc0bb1e64343c0b978fcc0d6e84d0d17c1c1f4093fac3b4c01837c6b37d189d7608f0c335eb38fe1f43573e0c525093f60ef618bab297b8a4d9d8c16":"":"":"":"ade04730059471b1829bec8dfbb0ec708be7b4e77d688ce7cfba9ddde059a52f969407291440aa79492f827fe1a2f6568989fd36b4fd84e6699152536bff15388af319fb306f07de4309eb92ba3da5f7007948335993698d398bac42029912bec6ba39226c2bf238733b5081aa0a2ca392a719385184be619d9ca56771d8e3716a46cfb339f93ff48abe406ef788db2ada45ab5fcb7f689bd801a5ccad855b52cd4bf1d6e338f2c3eac94ce9fdd0dd06632d01ded3753e87957e8569a67eccad"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 0, 0) #1
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"f8dfa70524d46f3545db3c687fe85a8ea35e32eda470b4e14b8b12f4e9c6bbf6c08efa9ae1df90ae6f14b895c342ae07b5e8d563199a141c34e709c6e743260b573f88186f40f800c4c0ec9f9fbeba49f103bfa2d62d7ed8fc9ff88cb1ddc5d4ca4d074e0053c069393d70a5b3f1df3e":"":"":"":"05f4e609b085d28958f5702eb7b99f2e0c7a80f095907abd5b7329628aa6dce2e2f8bdb7a2992261ea414e6434dc98162d02c51936542218a31c6072ed55c9ed83c79698de7ffd3835d5e4d0f3a0c2a70bef2b6c602d1e0cc814c71b2fb1a001fb83a0e2befdec7e4749629693629ea2397b299cdf491415dda446817dd7d28da431f95162de83d917f9e9325774e2f7ef02fe8067cf4bac47e2f61ba235b532af3aa95a6517e9f1286e065ccf9b3eefa6cab4c940c83ee9a11da55ee21c8d06"

HMAC_DRBG NIST
CAVS 14.3 PR True (SHA-384, 0, 0) #2
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"7ab7da47ff7a95ebf2367de0a25c7885d80931447d2f5cc73ae7f66844910e481e05f53ca993b0266b7cde89960d681a3d3c568d9a6e35347cf52d2e0ff7ad1142983fd7d2c848674315ed3e009adb7154fde1f2d90019cac210dbfc06279d48fc7c2e900652b5cb638c1260acd896ea":"":"":"":"f00714df243103f54b4c0c516a7a631431dbefdecc30c09e8e834f09882100c1d0276273568cc6352c3028c156371389078236afe57d00edaa226262f1a7f6e0011ba48d4b8f089cd257b6b7cfe80ca2bbeee99635c277254546d4adbf046935791be21c48a7882ef6cb81f7bccdfcf9bc430d21cef1d788d4f4df6bd6ef5bcbf48e35f116d482d880f597bcbcfbbf68bc77f591bd7346d7a1085fbc1c2707c17bb288ce6bfb0a78a54731421762f18142975b8b3b79dec0d852dca80f1638b3"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-384, 0, 0) #3
depends_on:MBEDTLS_SHA512_C

hmac_drbg_pr:MBEDTLS_MD_SHA384:"40e83cb1fbbefb44426350916b0995fb6a1c5394f2fd625774459548cfab27f2f92e2e889d3deeb33dfd6c40f610b71b70387af8d70768c52b36bb2a59f3ad9a16be98c726c2d65af457b2f7d81c75fae82523c977cbdf6138b1cbe5a9b3ad402ba197a3009dba459d3f534ea143e5dc":"":"":"":"52cfd4a4741b6575578a1b7aab91a366341cfd483799ca08b851bb0dc2f2bf640e90c1406fd09fbf9166bd55d46aaaef38e0449b7187d019e68a3b98a7dd9cdac63ae9c966db4d901d37cc147835d017915902621216bc1835d70dc2101ae50e0541f796bd6bca2e53260ba3353e6aa4eee56f80aa329173e347d83d050ddeb465d8e1aa5450e6e7eb515a92fbcdfd8530f04fae3d1a41b13151a4827f0634d6e80424c1e934ce0e2077f5f31fd177e9a42acfcaa67d4043fd31a8ec72a39e6b"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 0, 0) #4
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"39927d4fd0c3eba2044002e65b60d3994c3aad0c705bce2e9e41aca30a7c2f03e7b4968d8e729e868f5fd57b49a4b862b0bd169a4e2d77bd59745e778ca6fd762901ae3c0fcc48a0d6ee22bc8520ec450630055b3b66bdd2dde9f5215d241fa266d24342b50d42e2db5436a478c7ebaf":"":"":"":"96194dd1b6ac5efb3d4787bd1fb4c9cc32c29b67ee34369a7aad9a56f64f53526e9207c1d4c541c6e0df4960c54e10168284891841fe554adaa5012f325b3aea79fa4db8c36e67a0f914d9ab361d8ba0b3d6ca4904103f14a30a90dd6fd7c3f679c272dee7f01110f7229f4f5b6ed152a0149dc5a7185bf637d10899bca417cba8f919a2800d8a72d5575f0c174f98f77a1afad850334204e66156eff4572a6703aab50b850a8df498d1d96b1e2bc1ac34aa4399f3b13e97b4989539ca78e97a"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 0, 0) #5
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"ad10dbbedf980a0c33576f7606e14785b2a903788b9b7cb4c29cf74a8bbec877999ca28c36c835b60680bab9005d8e4f341b97213fdb6a52e783d19850906cb643bcf48c291cd186ebcbf0a287e459d1795e29ffb0c7c84b0f6dfbe219b4f85d9fb893c0cf9134263a9e6a36c76d02a9":"":"":"":"5db269714c4ab774c2eb14eb95e9b60c6ccaa6e90f9f879e295cc007069dd231894cd8fe0c09bf748e26940160cd0cad75dd2e305ed1f2527ba857c42c3d0662d25cbbcfe342910498ced309cda1894a1186ab935fb614646d299ca56f86defdd0a0f52baee1b9b9be05df85a05c225475a7ce1cc58ebc488a4f57fd1f983881754dcfe3bd78cac529e9945c89383e331f0177e721644b3a8d82deef548d161e085cff59645a345cf7af3f3582bed5b81c7de7a6a216403bb88804f7d16ceec9"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-384, 0, 0) #6
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"e9506dd05bac4750f5d5b43e0663ecba6444455ab6f662802897a493ca11ff05f76045b621004f4a88fc6b1ba859ae795e4846f17c3b1c127a8ef16d32381e27eeca77ec062a8a8f811f5dd7f90737147f5fca2b7cc89009b0350292b88d1de5de94e1e82bd5f7bf2e06882a925977ce":"":"":"":"abc3d68bb9b0d29655ee2057a60e59fb84afbaf9c75ac5d146a9856384022e4873a6abb963d8795ded5ce33f8df9275f8ae4c3da003797348734864 5415ed51458529bd7c4996128c943ddfa21484521fc645723802318ffd5191e957ec453a8e922d48b1e83681c1463a03c34175a5d610f8f3709b3044f45084f901704547e301f9807a7d92036e08a3eef791f67659816fcb28922b9b52e2a4a2e81cb848f9ae579cba346b0507e91f26b70d199acb6da5d3544b8caea762f6f30178636d8"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 0, 0) #7
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"f1f00ebb7cb4bbb3b0a083a290d4d3cc4db53aa9eb3f2feb1d428cf6d8104bdc56b2a30e75782693d7565c5d1ad6edd6cc22967eeb5f159989c2ed7fdb62103c055456f5e1a3163bfa034c502ccbd9aa75385d4777d03a82606a890c89a207494d082becc22efad8fe69c367fa9e3350":"":"":"":"6b75aa14c129d011191b9016b089af15b806a494e8e763a7fe902479155704e1a92eab48ce29fd0f1e9d5a2014757c3cda6e021defdb91c796cbad709658edad6c8f7ab6aebe978d507459198e0719eec49b1926a7c4e33e34e8e366966e0e4e7f3ce0aed6e51d7804d803a

ab57257ff1250ae8b76bfc48a505d4600bccdd992d564b39c3519db0c7dd26f5dbabdf3c098735688aad1af8525e8a6a343835bed094708b78faa300c08600e638e6f24f4b2b78df0d747ffbb9521cc6786b9c89d"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 0, 0) #8
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"1f3bade86f64dc0770dafd6a4900f61baf003c6dccec496856b7b08cb99db8f371f1c9606602ad397e0c757f56ec6176c04e832302fd6fbac3519af6d2cb9da5a85ee70efc19c7350145e904a7fa9d3199e1f6213999ee3bbdbcd1200b4dd4e7a8f112f3a37865e494bf8549349e9e78":"":"":"":"1a420c51052534d5d77347ed5751e44817824ed75467791c9717875dadcbceff2ffe024952958d4718b2b4028af83ecf363d57349a36476c0203fcdf4952794aa66b3692e7b0810ce060601817ad0794574b1ce12d6a7b6ec1d0b1e0acb2a6c453be81bf2d17e1fca7dc1c9ac5fe4a64069285a8cb9408051ba5ae4dc0c8897b4a216109b22ec56aace995a453f28dd7d2c38c7d44739b9f09ca0e52d62f204e7f4a09c3e231c8cdaf54f941e8d5565b25155be21cb316417a4c005f7e834d0e"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 0, 0) #9
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"1b288c94a8aa7499850d7bf82177024f20e8ccd502b7b0f529c47185aad4eb82ca1efc0104f93cc35885e9894671b9d74fa8237f5d740fec09e90b88bc75124e564f1f198081d51c950dbef6a6ebb2b5e1aec008d8a5a4c692f6467c740f5026807bafc0710dc8e9197aee4372b429cf":"":"":"":"3daf72d94056e6c7138787004f40a4a0c81a244c8aa14c332675e977330b63315916d8fe6ba8f0aea5a22def342d4136d1d6c787b3a6c6c05a44ee1cf9b2d8911974974cbf7a14ed5b83fceb8dd8d3ed59194d3fb6cce579a97244091731a4c1ca1d6e4c9d2623a41de665ee3c8236e0da8710208cee948f248329781f40f6f4b4010508c219755b6df752b9523ed0c9644b17250bbc88b4338c688e97e952a924da894fc986f7e807fca4477be94dec993cd6910709d8032fd3a5b97612cd65"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-384, 0, 0) #10
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"1e1837b46486b6e65713327240bfac6c618e817787c277b995c92dbe03b9b01de8e100b303ce5bf5048dccfce4d240878ffd5ddcb6754292291d1a79ee1e62b6da6b23d7a83d0fe9e84757dcfa51d05709d54142b42dc876506876b136b6df34b485c0c129581972bcbc674b893ad61b":"":"":"":"23c258b93d4e9943783e88b244a52cde6747d8d7ff28b77e2ddfaa2edcbb29eaf41dc75cdc2c5b581b3a59fe20e705223bdd90e786f6c6498330ec9bd7ca7303e53c0b21abef1497210f8222850ca7f01e0af4fefd36d82e711fb17f581b951e949876a5ef0a212fb73af4d32f6bf9fe8c9e60849fd2311f3b5cb8a4abe856b3dd629fbac41e6dfb502d1894088fc52832cefff807555457c03ba7b7daaf02830d9ff8c9e8ed09ddbb68d6530af0cc5ae9383acd34c89ec189f5a97abbf3ed5d"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 0, 0) #11
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"67b2a6e09bf31ecee8fe9c719491baf3c6efc0e27519155f99c94667d727420265254ee6d34c6b9c03414452d68929812f1d23aca44adfaf6b02f519dfc3f034bc32c1b763a129a97c7258e5e77ba69d6eb459be2cc96fd6150b6040babcc406143bdc2c1862c7bf6607b4be95f3151f":"":"":"":"d0f71e56e975e443bd7364eaffa9dbfb60a82bd0ea6405de0b1301911449ae6ac0dc8792acd2b0ca3e68c2abb982362eb2a7a8f95d2960579f9932070c9cd7abd57a36759b2c6f12e20dbda8a16a17c29b70f5bb8db0efa9451d9a349b9917b7bc39af6c6be8217e0a6fb52e6a4c46dfe41e6a9cfba84335d0254cad07557fd7aa3fea185c8c88a921ea665e410067395791785ebdf1793038ceef6c590e64af00ac4ce69ac3d0b497feb93b4fee7d55cf0fa40dd49ea748b33f038b5097578c"

HMAC_DRBG

NIST CAVS 14.3 PR True (SHA-384, 0, 0) #12
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"379d0a38c8897a6524d6a59df4f09ba975c146be7a398c3cbde8c222fcf998102e98223b81dfca7fb5bc92b164afbaf50f58b8df04889dbd69acd59f7d5ac08f81984910ee20a4d58c51512a3ed893d7b736da894a0b52f75c5208d14f858dfd42290f4181b7aa249097b93fb2bceab8":"":"":"":"166f643609dcb8951161ca15b3660759b69da616b45761b8cfec01a8a7f51a0bb1cf256c9fabe69b29552f8e861cbb3160b905d24845d368a17ebf911a839384c3b3aa6c8dedf1fde12384ec9535ab9d008728978ca58ad88780cdc3d272d1dcf2059b9bdc0d2311812fb1b559e31f8e5a89efcb2b33c705555ee0efb23d2c4d312fe02b998eb78af85e3839963afd98c1c644ed4493c3f1af0cb210e660748cadcfc9ef85fa3b5fafe345756ca34e7b7f88d3aff8783e92da00dbead5d51f89"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 0, 0) #13
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"96041c211e97d480d149e75c876886a78fee171e0f395a952a0e873af4dc22b46cdb68a60dd1d5753027e544643c5764cd65e202eb821804300ea618e8ff9785f3bf2fbf1b1048cd4450399e2f642af38bce41df8fde3208055e34d356b1aa1b0180673e8507af2035f75e9fe629f979":"":"":"":"51475ffba32991781b17e38ea58b08bde40f03b64824187b9506153f41c233f34dbdc52b63cfc71b120b4fe6c2866d11e9aaf44f82deddaf998caa56a4dd58a6ea2e8f5e3c4ec7fef73e5620cb6a77313a4bc0b135c57d18085010a4a026059c2abd4b6d2048393c5400341928f5ee6c5a063d679e185eb9be2834a1009d03d298b9abb09f993a8ede54bdc4d9a95c2af5552aed9fb02cf598a18b5cfe6c811d1ca4ed764d0756fdfcb5d03aac1ed80fc86595539c105da6b66a00a91caf44fd"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-384, 0, 0) #14
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"423cf6fb44605cf03e3063bceb92c156e38c5badfaac35593139df46d325242c84908baef2f824bf3ea66e74bb4127a0c5650c33f68b5d33502b1f55e06fe2c1169fb34688a09291d1e12e5390a73da125be4cf15692e3e6ad0ab6ffb22cf3f77b00333517ecb2239c9b81e59a72d087":"":"":"":"41f335cf727ffec9ebfe7cb348d11cdb4e5e49a9a047d8342a6656e5d235219a5d80715166698cc1f16e34f743811b820e6ea55c2bdd0db1b97ea2269fbf60c739feed818282f447bfe2bd0b9a7c479144f0016703aff450abbd87a50e5e5af0d2d9469175542737bd116de2a73acbb74d9f0077a227704f271fe0696f071914dcb9c0f0191fee35eb66248eb17991b538649457d5d5f9d4bb9cd81c33a14d2becce003c143c9cfe39ccac51048ef169f6a22143eca721d04f6e147749a44a75"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 0, 256) #0
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"0b2307c32f34d3f3c3d6887fb17ff68b01f158ef07438a41cde27d2d6725277f33f60888aa32b9b7406f78f47bd877a1795496f759d693f3f8bbd65cb5b2562c4a8d4a717b6bb8eeabc4d8f56118a97d3787d3065f1e20e6d71a1dee563fdb2d56561128fa83d8602fe0da3e89b019e1":"":"16815bf5482abc969179152f79aa34a04c28d483e6ac81aae14f7e0e051a5662":"938c363df2740ba9ccd39168f9bbcd7d421566955f141e13ed039c4d86195392":"959517e0b27d461d678ba2dd528bfb7e844f7bf14a15fb176efabb3a5200ff2b373c7c0683f095798951dc7ffd62b172ed814954c44087fc7a6695a5a275bc8aecd3a2ca8ed631a9ebf5e1d1c515542c67f31e16fd3ebc7e2333c7dffcf385f0d6ebe16b9ed42994be9f83d0cc1e2b3b5773cd2963639ac74ce64a311ac0726014bcd213818cecf5d562cd1c5e97be4028f64400cff31fcd587a004cf60f03c6f3222e4dabae5c4bdef8819670f77f9227eaf55eba5238f90c4bea4f03588b66"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 0, 256) #1
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"062f2aa7b48c983c1c6d00d06aa523a67d4e86e5bd266451bb286dcc5888

f0f4940c3b022cc76d68e1706d62fea84d052a019b921335f69ed5dcd902632116759b68e09b531de276c9238faf3a980
2806750454a5260bd808b796cb12116354b9a7ab9ce33f8dbd40ae7e74a07cfca02":"":"4a217bf136c3894ff7a3ca07ea
fafa286fafc8a827328b105b3a8aff28e49d14":"e433460e9414b21fc3d5e2705c08a21a36acde4458e24b78dcc51199b9
7c7a9a":"5c980247a1fa16ea086d54084281c5fd114777ed21478beee9edb175be7c4066b197065da5f4c15750783039
eb4b5e2cd4ccdc2a45c49ce535f03a36657f218fc616b3e8ef0c84b78b0cd1c57477242bbddbbde098be573e20d6ddc76
649d706e7f6c7ca3f44c845c2c9c9d316ac8b7389f7264c6f8cd6c56ca5503e5b37f52d19e8d47cc85a04a0196b938743
3bca3c18dc30b47030fd297705101826840991eaf5b856a5ab75d2bbb70cb13e0dd1876802fc2bd776a518b9dcb9484c
499644"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 0, 256) #2
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"0fc79576bdba77a815108bc9cd2d168ee30f9ab76db70600ac95fc40c1f6b
724068c12b99cb4928247e64b2ea8e75c728ccb3de18adfebe24ef99e14ad54bc1b3a486891b00b1c55172d16adb00ae
58c9d8ae0fa9809245a56c9118048199767d35c026e6664773562af011c2ca7025d":"":"b0c200b6f8548643529fd414c
693054d4fe04d8f76c3fb8ccc6992ffc25e6b19":"b91bf188cbaf4b01350d726585c6f3601a26b3654db2e2690a14f198
9f83ad85":"7c64e503eea5b3df44dc0eb986188c312a0f5fe1f113239984608a69ccadce8a7c7f3136169e075b0c61812
b1e74dfe6ab2e7d6f247f73859da5a1068c92ef8e6aedd94c3904b973ab887ca3c38de70b8b312e32a702710829ddf962
f0e08779ed9770975536557e3f912ef0d5c4969202af50252117eca8182c30389c9b84fda95118f8c748f0b1752c1e58b
8e0af530376aa34cd874cf49628bebbd7353ab4a5f64bbc8e3537762fd5556c680290b2c523153432a2e0df1658f2a550
7a30a6"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 0, 256) #3
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"ffde7e2726e89cce816ab3e22572fe31434f3181d0578d51161cc77305e25
62b755008c7e4ccc8ec62806bdfbcd8508ae418fcb0b57a4d1007469ee3d959a07e949094b0a3e5af69aea3a90a222630
978af9139027a656151225a2183b92e980fff9ba9876824bafcf18d63c916fe7ae":"":"bda1741b0b39d9248dd0628703
34e33cecde5c5f63a07a3030f98b021c6849fa":"1b5336fcbb0ed183e0f80cd31ede4f324997ffb842a83957f41d291612
c55e8a":"61d542e4794e9bd4acefef4b325d954c8ec6a29138476ab1bb037507cf52c17edbd511579be5c232a67269ef4
2364cfb4e2aaefb31d9e8e260a04e51d95c2ed6c5e0f095efd92fbd36edcae4393659af6bb98b0b71b281e91e1df37c353
987a6a9e259f2735fd16b8c1277df651b26ac3d9f292c9252be7fe09ab7851f515325a078cd69a7573a4810ab460c4c9e
7604e54242ab956fe471e90f86613ece7372f1aa934a50dbd0457033843b887c279f14ad6b4960f401b7fb777253ca5e2
95f"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 0, 256) #4
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"7946fe7ada4b545090d7647c99f71594fa094593115c23888146b27a7ccb
fd77ce305c1ae4fddbb75a65dba4f0ea18897bb7e9aff3138ba030005a7d1c5802838ebb20848f8e81e7e8018cd0d0dd9
21243c094aa710f6b0b2ea004bd684799e3caed8c3c8944d5da995b88fa071d7526":"":"b29a506c7bc8b22825702232
30664193216dd47f7d20ccdd35943a88c58c0503":"3a4c00cd2f278f0e82498d33fb6ae9e020f4d3793e832afc9864c0b
7b6cda43c":"8c0667d913b13866c7eab98471109d966901fdc66fa4dff8996ce81ec5185ce374b118da34e07bd82833f
20fa4e44ef159f9b0c47c046307a484b3f52822a596bcfb49b555ec8d481fb30e13dc9898f093d34cbb4d696d70161315
c48def73bb1c8b4947c8ddab101d4918f5cc00b890b7450e4e10c17c46ea7f5e0a1df65a1fe74ad2577e592e7bddeadb2
46fa62cfa5bb8620220b18fff296a19a5a3ae6b833321ca779b7cb5b55658931610d8b7776087c41ee4d077400753681
c7da5c5aa"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-384, 0, 256) #5
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"5459500d5a709b88bf067b4c390837eef5ae2e5f109c110a84cf32f561d26ddc567c5f4cf0f418cbc2a56d4325b2727f875cb1ceed3167136f0d93940417f616a3843b686ab4f5dd3d808801054c510fca5ea8fa0465f9d1afd8e0c68affa10f5af61e594e66b2bdb2372caa0712bff1":"":"eaec7b75ee03cdf0508c0ca171b005077954e2cec7230b0aedfe32a15cb1c855":"cdafe409b871625ab1b06a93c4d5a1f8196777370df18643f97050d7756adecd":"486aa4063b3840f0417034c65676d20da22c510d281bbf407855cb58a87ac9b33511d692315d88d27bd5d1ad5c35ec8b99018b5ca64897aff48544a5e578124ddc00f785deb60b0a60dc4873fa9a148da4dfa1557baa3aafa22680a40f650e4992d21e35fab3be5458dae13eb2caeddd8704d662b221bda01ac6329e2c451e865af9701a7ccb69c0ed0baeb226e6fbd2b871b99420949570bf5fc61c673aacb58feabdb304f870939d705426aae55cb3a2f3206c33abd453e077c4565c603a18"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 0, 256) #6
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"7e74b0a5413ee2ad8de814ea1f556ca5c54c6f11159f1fbc78faa86a74c4871a11658e917fed348e779aae510d383290bc6c4f13391709f8aa9bd79f38f310e2ffbe7fb1be3e6e3aac9d879f1e5fb3eb1fe81675cbdd098cd287f66fb9b28d50e12a64b9e08f28a40ed446fc3a12585c":"":"d152b0aa1946cf177aafc7d47322f8c756831550ec79adb40f34681fd6b3840f":"152229388caf5dc50454c2514d9ff1a4b70e3d1d9b8b29a228d59ce67e8bc586":"a1e2046729e849482bd693e21779e18370a542e2fc7baedbed054476f35447e069bfda33fa2723ad425717c027e8b30d57dd2fca8cf268849358354478cd8bb42e8f9a737c2e3d5490991e4902a52e86d1bafc1751f5908a36afca2b6b4663ccc9f1aa46e857e2ee61e4dc19d154029da48d59519dde64410b1d7daeb5b7b93213cba1bb059637023f928f16e5944e0ed2ca07be3674fed6e0da72313b3cb80b7a2d6533fc8785587366ca1b6769db803d6d840c5d1b6c4589272a3fe9371b0f"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 0, 256) #7
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"70b5cab63391c5777e4e60516b7095dea3cf26d72b27c19f5a08de6634306d992de4c3f70bf2849a4c3dbeafb163f5d50dcbbcc8e6f4bd973636da95d71d39d6ffc9e67332088bf906921b9c48a7e3de158740a9c0f29a7b69d5545e390030965e305ac1653958360d01607bcbc39fb9":"":"ab042d23accf9a9473b43e82683e30f436fa492ba4a8911e4ed2622d481e0cd1":"b707e2d5a5020d37656009713bb100c55819a98e220fbdfd921c6c0724ba7238":"f3f82b7aa0639bcabecefc7b07b3eecc9962884250fad11b9351226f138e06e3e953e052792d0127618a28aaaa1bf5374a06393c18a326f8d3471010f9840dd16ec997f53fb981aa2b689bf1cdbf265b4ab698f9e8e9c054255147e04654b8fb1d0fd3a0b64d3880ee6e9fa87e0184f6ba307f4d3fea651556e0baeeb75f308fa32925f8c55ae0f355f8db8495ec6c46003763ad4ef36590ec40239b5e8530aadaac931feefc8e392c550ad4d89f5b314a53a0633c7a93bc05b588273e6d1d56"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 0, 256) #8
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"c17914dd6b73d65e5af112536f52b046d4963f9c9098c77d9dfe35ca7ee6366d4c0fed576ba4cd14caa3d0c406fffad2f0748362166975f5bcb9a395d568b8dbde3383c5654bd24f26890b21ee1f1cb10f3c93cf2df64cd764187c840590a54babc9c281de88ad1a1dbc2677fa8687f9":"":"4a61ee9349d53f8b3c1af36fe0a9303ef89705fd87e06e5f34b61e1350111279":"a9ad1cad4ca7a5af4bfb83680d4b914c23a6cd551e8b002c50f30be0d8693edf":"9ab30e3729dd8b2af987dcb793d7a3e1fc4ebcfe0a4ac976d91bd3897777effb210c8076e9fd135991e54abb4bb8c7b183a80ef37077692e519d38df4a04304fd83fe1d67d32147fe0a249a6c8bc603d99878039b873588c3781a193437f098094fd8c12945ef99036442c80cd1f544725040df980c548f0a675afaf62a1b7c225c9cdf0703e613c7a5d72c8b00d

8ba199b8ecb48b6e0b0d103a3b0f57ff1a4b9189a20dedeac6eb26b1f66ea0c34ddded10af2b0133f4b5b95ac2239dd94919"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 0, 256) #9
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"2aa5423270d0859a6e3aa3069a88f3ac4c30eda7f6e52aa891e4f995244a80d73d73f789561b00ceddf721ea59a7eda3157090ec192c578fc53d232c36453c5e8bc3c9c22f3aedb6a93f7aa63975d9bd3369cd518e570f6af0ab162e4c938d17dcd4f3ae46d7cd502ef73b2d40f50e2a":"":"32cae3ff757b79f2305a8b5f5fff5a77afb581faf5a3796c5ed7054d7c048017":"632eb6f1c827cf299f3403bf80af721fe5ff8245331f1ccfbb8f4e61ef5edadf":"1a85c36131a8c271d6c805233098bb29f9104e6254e0680c6e264a76f79ec17c7ac65c8a97610a0a7e5304b37d1ebdbe02cf9daa9e45b81d75d8c613afb974eb38dc49041eafa7462b4c272fdd3d7fd4b05b1e6142305ffd6fa634ddde90e273b51b02c0b68b823c77ddf3e93a2ab9436d0f4801f08a113eefeefefb9592683981423f83235f8e563ecdb4e44daa9afa5e1728204dde1bd254c7985e6d56897c570b0c6307fd49ae4dce18ea55eae846af2a5acaae17a71f8369b64f47b0e54d"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 0, 256) #10
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"c69c61689d1f7763d43b22b6bc2262c377c62db60835114442fd5bd65c665705b5563b3b6e9e793d0f4128696eefc5ac603b3edb35b705ae39845cefdf8fde23f5479ae4f033442aa958e979c89bc41dde68d92f05b28c3644133d19788624bc970019a10f6b3c6c5b8dd22b0cee3e26":"":"15cd6984fab6ae7db72a4c099a064cdfbd141dce361fab0021872c91b1bb65ff":"86c295fcc7f9c2ec9fad377e0e4d0119334080f59fa68c21c19d7a1212dce03b":"97b971ec13db049ccd72bc597ebc2e33fe4da647d0f74855f242884d35dcf92d0349fdb3527c87c5431c10fa85569285096d3369bd1917c8c7c8650024acb88e5b17c42b50a75419e29757a9e1ae09053cf0b51dac437883cf3f5b1abb40a71f40d279bc9d596d0f59f4c70f81087b4446c402279f4486198ee3294d0a5f72eba7ba52cd552906371aeeedb47122bffb0d5ed27c3cbb86a6fc2d83ab4db7b6e1ee467dd1ec20dc15bcee168f2e200179714cfc04eac651a495a718e1ed985bfb"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 0, 256) #11
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"4dcc7427dff46b7db7e2d3273e0605ce85c460cfd4269fce9ca3b10399b99e178b12f28786b9e3df457ac0015004844d6f6bef29ea562856ee82246d24982393f770d0b65d0ffc660d9d8359f10904fd8cbb76e648df60ec43237ff7dc46bc34920bba637a2c1643a53e8a88bb7bb97b":"":"4c0ab67b952186f2f85a0dbd4b2c1b0dd009dd794260ee7f321b2d2b3d994e09":"f5be66009b79f51f6aa0cd1a5a24a72c6a6c4263263cbcf80e8e0d514a2bbb1e":"211ca57a321cae2c6d1ad755ac924c92dd09bb1c6334ecc543ba78a18608479457bebda63f707fc28190b2d56e4cfd96d8c49fd146ace867236c57761ea28326e3d241d1dc35d7ca971df9d292f2563d33c5f32abe86367cf5f2f06628376752b353f72b501ffa94a50f146b8174cb7946ab8c8be382237334f37594418850a233c536d72763f10b06f728e3e60d3b4f0377d51b0de11d110a28b6fcb7c42b77e5f6b771c8e5d713a0f6c4d82ab2311cadf16b7cb441a417b2f595f32ea822ea"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-384, 0, 256) #12
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"b72f34bf8209a28168ae7692e4c7d6f19feab9346971b85fb9f377f6e4a77dfb370a10addae744ac03f2f277c85423945f486830cd410f26e22c23a136d41800850113339242e1a0550bef81a239a289a8d020c14298854f0b17abb0bc461ed6d39ab2d9cfb03b835916c2a8e93710a0":"":"e919d983beae4b687bb393d90ad4104146e86564845800ecf82085d5b269f1dc":"abc8b519db05c1de8794248c5741627cc00ee35a972ecdec045a0cc557a2d967":"9777504473adadade14eefc0279f8347bb178a36dbb5fb028f0315b4309fad4ef554bf34b04146ba4bc260

a89cf78195ad1c23c6e473a14385c66ba2a1c005cdfe336999245f00ffeaa41dfa3d9e68294e5d676f01f213c6d2d8a69b
43e36f2a568999c0a8c07e96d7daf90f3e2e668eb9fc8e5c812a49a39507d193eb7c95b947aafe658a1065efe9370cf810
14e4ffd54efffe5f863e6e4b7d875565617d8b72854ecf09263c55d1c3f1a4f4862214fafe7f03da5572095a7befcfd8e6ee
63"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 0, 256) #13
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"35d5a6cae5aefdbc62f1efb638c15dda387a8f651810bf068a8d92601fd37
e0efffd95196c09c668ddb05eef3de339222a0bd0d3b721a27e2f29be84a846c3964eb9a84cf69b214f612df3b414729df
499da4d3ad8bf3613bdad3a70c73cae80556c16f8ab83adf0f2bc9391094bfd98":"":"cd603812a8444925993f2c1a0691
bb4459faedd872f43852f9970675f579a1eb":"1441b6d4876b050fa4d969f1845d3f119cf5d8720c35da9c489000e6b71
65db4":"259828d05b8e735fad69527cd2322f94e8e7ac2791607ccf2a74d070bf7d5574ffd8d6e447cb4e02bb15a87aa8
8d8f1667edc0905455b116ef7f08ce727d8f266965242e0042810f946e52acca6348d70e012d998322a18a2f3b4c4c6d6
b66cfe65385312344e3eed14c6e7277eac9a4d09ddc5dcf8fcce6f79a23d34c80cb78aaaf1347ecce8c13efd450d595065
13e62f527179b95b9b5d9df821c32538f8e1ccb17e911826e944ec44943ad8e726d54fa98ebc4d012d34a23771ba497c
a2e"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 0, 256) #14
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"66abf17d907a134232faaff93bfe361223b5b773980cc261fd19caaca022fd
0a081c11efee01fb1f7abd0145b32a51b3237d6ace877ca6392bcae2fd2aa5b865aabfb1d1d1da33f42319a088c8dbed11
24a71d39e627d5efaa1e8f3e5f70114bb03b71ce54e4f8d34e838106b2467cca":"":"1e51f2b67538f84440912c6fa20fbf
009100fc3008b5b8e1308d95e7ca53b460":"301f91c659f73b618cb46a4343772f1eee9fb4949ec6328109823749bd8b
0b11":"34c532082926e6d530b3a58282eb4666ac7374e8befaa4999dfc9f409e40ff966652295d2940db97061800583b
c7d47b053553ad29c89ee61803c1089d30592270d2927031353592d4aa71f59a4bf3f2147cb406322367544c38fa5a3c
8ccb534bd884355b06145db62161260162091c795874a2e99e01292a2e39e107738818a211750f858edbe0c2ea4734a
d14f1c45bcc9f733f027616926558587f7332be55044dfd6fcdb628ff7d7d581820a217bc64aa092e450722686e0cb291
eca45b"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 256, 0) #0
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"37dc21c72dc7c82d5e13c51ecaf5a8ae06402500d92caf96c0555a95069f4
f0144a961ead5d6d9bc317afc8206202bddd57fc02a2a500df1fb5c4d9d8837b52a5220fdf068fe2b8b4bcc63fbc9bfc94
c8e21d987e8b6cb0f4cd37b144c668f18b7a36ed4e9758ee7b96029aa0ab2196a":"41e3b89347bd035bde510ab8ff83d
5fdcc9d5f2de648bdb468a714f2c1083c52":"":"":"a929ee23c5832e5ab93ccaa40bf775593d7d04a1a8411dfa07b4c8a2
da2dc91b1bcb9c27a0ba5a7152ce5ded5f76cf6b83c04c0f8a4f6b43383ae3e7d497280c0f944be91b0bca6a56df2d0064
1bfc1ec549b538898e559407b076164278c0eb7afb6d6f4495a50d4da178c04b259d21bb745692d3bd186edf5bb3da6f
66b4418fc3d9b085b0a6c1a5e54696272c305c4b8887595b391dd6ed8da03dc9fdb2728d8c40a2defd8af05ef1c443a72
323f2e0b0d268109fb7e7ee70192fa06bc6c2"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 256, 0) #1
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"0dcbeb660cff703e059913eebff4f639a24b611a078bae8f01320ea4af5e8e
0ed93b8dc4e84d224036b5da645c147359c6123c54cc2367262a7594bc9a7dc69f76549ab803af66de8f253d338d48ab

827b2b1918d636d6ec92bfd9123f1f5fb59b6c37eadca0ca7792e2b7932e1ddc33":"1debeed9ba5790437a6c56dd3c9e2f6df0912aa0ce2e57fa8eec9652e2eccfc1":"":"":"5bd815b3c3bb73a45dba72c68457ccc17212af905607d827e8b5ddbffa34a058ec360abbeb6c8ba16c770ae4826135ac7e4faf208da8b5fe3b26c16fa7c7ef4000c3dfe1b8b707dde64b415c671c4615d56e2648908e047ac978a389e346cebe9228daa7bcdf5e341f72c3c7ff74672edd60c7c6341726450ffbf9e3e7a16580e7e602f9ddd3f3556129052de05991907d81a87467ff5842c6e5dcff4543e24ee48149f16e9107a9aa40cbce367d4b76042d77ef1790b0a7701b2f04873d245f"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 256, 0) #2
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"d9bd99128fe2771918afc6db6b2514eea0b617d9bd4599a238d9d99a7ce18995e8d85542f3f9dd89920b0f79b94d7f551fef4a330e9de24eb197bc75677bc13d8361104997af99ea2c6da03f4e71c89e03191bc5e320f057afee98e98facb99d15142c61ddd71666cdc38146fbc3ea4d":"eb701a9d119cc6dc0d735254067dfe161b1052ba3f93ab0d6bcc19cc0387027a":"":"":"67b86213a84778a9a38eb9913b9db8508b53ac0a81ff85dc78c966d638255f8f7c63ce06d4a66f5d9213ec2b32f7e63ce5dcf01b59d3b30433f0cf4c06c171d839953de913093ec845670b38ecacd81162dd73501b2e4c2d9dc69b97d49bd6d9f6250070ef6b360305fcc5ff392d1adad98d6bfda67d10b725c7cc8ef6b4fc206fde1871712b96dcbc2df4f08d79f1adf7fbb01bfd8f20e76956ed4b9dd1d7e5fb4f922ad2a529bd871490e741843d839e876c4b475e2fa140f28ac8d347a07b"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-384, 256, 0) #3
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"0de3fed3b363d20ec5018d4aeafb25c8e0e6aa42ee8b56843043f8d9c40b9bdc8ed427d29c469d8976a5b785d050f3d2e5eb287a064c54311bab32dcd5f240682babef59c6ffa602669f3ce4590b054e2550444f249b56666b7b2fbec29b33d1b29ee653e388f9fb54b00635ff526dd9":"82b6a44b0f35f946fa0fd4628738e61a0bdd421a8de73f3d2efa25216c789080":"":"":"1f7b951d147ddbf21fef9d4849044c44b757309da8f0244f71e4d8301e1fd50c5e46407f5bcbed83eaefdf8983c330dd0a67568e866b20b48c2bc97dc63a7c0d3eb60f2488b1eefdfaa7b8dd43132511b4a2ca80bc9e82851584ec4ae463444aadd3c8e6db2d4469ad9750e18a31337613975b3fa0629b9a22bccb235d20157a4427acd619324e881e68f5615c65e59a566a73e4ce9d484fc5b0b29137c4f339be84781cad67d17de03099b1d03ac45106c1f2eb5b380ec84392b7ba5c91df4c"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 256, 0) #4
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"abdc2ac24ba7d92ed9f518d9576510969f8d22074bed9b7639299d2137532c50faa49b5e843f417693a2eebd0ffd3f27c0ad2d8bbfdb912ed4d1ec85165d4ae577a92b1affab63070e25dca8bb1b035c8bbc5d3a07b4fe094690e4a45b99f9e5bb6b0bfe823f3c2a148732fd43db5e5d":"8c7b18ce389664fb72e777e70b533ced4c04b0c290fdd45b86b6b95708d74187":"":"":"c3d1420055f71a43264ab8da92829fa1b8937346375349d2e256705d933a21352ddb4eeceb36cdeab38cae58da81bcbe6deafeca5d7f018a0514bbc285f436b574ffac2547d26a3f9aef21b66c1e70b45d372e4dc2281182ae94667e442f39e1b9b2fc2aee06ab306095a904614613b513cf1af5a9df12b996cbe88cc3b25401790034ad0622df43af4cdbf9cb681538c79189a8260cf9c35378955f2ea859faa78773854883cd94bde4c0f50d4c998c278e47787e3f74f3dbb98f710366d315"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 256, 0) #5
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"d20353e175f4ebd0ef5fe77f7f6fbf5340ba07934828dd296c041a63de841002db0d21ecbfd5eda2bce80bed6f73c23d3f18900bcc02791ba9cae668fc33fc60ba84c6eb40afbbfff18be5c4960ce57ad67dfc8c1eabe61a299881c0f326f7093c1a232c80467772e707dbe75b5558d4":"f38f23461c471181a4179323aed247

299df11ce145fbab9834b85b3cb42a10f5":"":"":"76a4994edba3d0d9ffee9ccb7e12a75e79c5ec1213f45ca4c50ad629a
c533e5e6dbf58f8fac193755e74f9e7a75eedf89472e91d394e32eaed86efa4fb2f9e7fe4bec1d9c7a30fe9bd17c2cda73d
136e752a9b818cee6f1262028031bc09cb81b89156138b571f03afa69dd388a807a8cbe9c4de66cad764114f9a4a6419e
a70ccbbbff9dd774aea8a2d6b1d20d0a577c59953661f0a87b4d795c2626a025d733f43bb5cd1df37f5cf542c7c8b6bda
061cf4693e0384060e63090415d7470cb0"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 256, 0) #6
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"a58ca5154659ba58fc1b468c909c667e1b5087884c01ab15f86fb5a431e9
82c1c041be0aa014fb310019fff65f40ff13d4469b123223ae44f4f4ac0fb6877a7890f969d39047e39ab23882cd7838e1
6e64bc361fe18136471dea2e71a86ef2d9f8f7e1d24643d7df292409ff8cba0f13":"dc05980e40f07a02fdb150af580a7d
195ba26f4fa72a1fe513ccc2cf6e4f699f":"":"":"6ad4543c218cb6aafe65e6a50c4f9ee9d5c7a3b9a0112bce262f49f5b0d
20dab7225fd0acffa25165729d8fbba038eb65f7e72f136e5bb82e8d94698dd9b763c38f3041ccece3b04189aaabed79e4
d4213e24218c5fccf5f9a0c3902875564431f4d670e6e60e1dbabcc4642c3ef895c115e28702927cb98d509f9341ac7ae
2c6ef6c2dc4537e909c81a9804057b6e24fa63ec5edce835e624969a969e2c47c6dcb7e9bcb2bb8f344d2b9855a43e26c
0606466887b28b67ffd7f99d374812d11"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 256, 0) #7
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"9d6e99a11d63cab5aabb1462abef66bef31a2886cd172651bbf30f65b16fb
8f3b93b5042a908510d8518330538a06253959da557d2b390c6fe0b7ac6b18591e5791d275c7e3d558690719d5967d0
26a80604a389946e2a55486b5c49c2984990a2e14824aa2922e6a59892c5e6d969fb":"af631e7990394889b84d85192
0ce8877934e706b780908a07211d45b247584a6":"":"":"9f33ba9083c7f4088c9505622cd5b4937b7189b0cbcdcf352c
54ef72057594b8568cd4b13a4bfeb61261d27f5febbf2cbbf902a8d55f6bdf669238ae84b8abc58826841f7f62a0c5bd9f
74125cecbf8e3b4c1ec88663114e7c248c41cce92e73b05eb3f826100c1b2683cbba985d2ab694b5de1ed8624628917e
c9bb97733f337298c0459f198c7a138f1670dfac0d58f287b8244f0605f97406ef528099aa2ef290db202baa7fb221a852
3344ad836c9a2bb25e1ff3fb4dc20f69ebc9f0fdd9"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-384, 256, 0) #8
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"df7c57519ae3914c75174b3107b7ddab95df936c5cd7c296b1cb1ea06249
915cda22bac19ccf2d522137989d5a42549809277ba155d04b3353520f4b5c2f18120bb4b8442130db58e9d46a1a41f5
627c40a6b65a4f9075460b7053202a6e5b12b9e07ae6ee9b4945d4235d0b736e88f2":"10a198b05830cff2fb4f5b0317
c258129396edb943769292753095b58bc8fece":"":"":"17b9fc6419c17534ee16aacf32550cbf58ea1f073b8e72fb9ae6e
94094e797f216703da428394a1da8236f725b191cbec11531a1f87946c70fb1440a55be7d7d18c9b5085d626dd0cd9b3
bd63a9014e5d14eef636beb694dfa7f781e83f3c1b4fe5519ab1a505d1be5b812514f3a39814601db104afe5726086f6ba
cb61c00ab8210239b2891938e97fc53de069f18a6469999727a904403bc53c6c73c7b3a5f9f37f380563f1281cdaa1b4b
b4a636f849717c307848748172ae0191997abda8"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 256, 0) #9
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"2e403c307a03d766b61001842f85caf91a5eec97a49934547b2ce6341191
6495f3e102d333269e04381bbf140a28a2d61fa6a5f2286079619f4f4fafeb5c520c602d0ac3190fd500a3402e7c0647ac
76c901e7c58e012cd6b9e83d2a969f0d0ae4e08ed5cb601fc72596a72b4854f246":"ff1d9eed8cf59f5708e41924cf13fd
5d30ccb7dedce3062dfbb2c4bb4d36b65b":"":"":"e5e20f2cb063c1587583a381536aecbf0b0cb4400c99a74bbb6aa15f

338b3e67187316865cf90e691d99466e34bd6612985575122c6c79848d4e2f26801d98e49c002f4063019394f4b3eee9
08f2d6b56749c260e56ece4e0431650a8bd9735879ee6c9bfaa5d44c07e7ff6978883c36597c31126386dafbbe0355798
19068bb060348629f74420bd411f2dc858d46dff0bb4f79946af96046da2c2cb32e0aaded4eb1ebc8748f277317f9ffb9a
adac1bf5e6654ae7131d5ee0c765ff3d49d9e"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 256, 0) #10
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"4b1240cedb84ee3f395317e177efcf03b0fb57be1e01e3c206170877a06ec
2cc077e9751b4eec964a4422d010ef1487456fc16b3e6e7ccb8a06230144535274215f00afe175d394cb04518b630ba7
255ada0c6676885801a8f503c55c38850de6f7904b40cf03fa195cd16ea2999347c":"9043ef3c775f32dce1902b9efdc4
81f61f29220eca53bb904155f2aacc3b3706":"":"":"4facd2fff1828b9f4a63f639503cf6533a4d242f316ef7168fba44b5
2b876056bb0fd040d5e331d2746169cdc88ccef74dcf6c642c1d1a0db4130f8be9ff88555de4c2a7a5824f005cccdfa607
4df3385672eca57a45679d69dfec232cc8b1bca87f6f9c6cac2f630498d52449a5d1b328a6d2ac1a9054a0658be589bc2
77b7750ab5d647a73a15a059d72608f9d299d11f9fb417a37ddc1b52c8b8859c2949e5ebae650b9cf8b4fd771288e582
dee38178b154e681eaf74d4d3f35daf00a309"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 256, 0) #11
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"c2027d8c084e2c6fc5d535726312bc6362372872cd37bf07cc1c3870f3b5
9a970c62b84a10d1498b2e02027d854fd84dd615e29e7c204579968569386b6f08393322c4fb36da4398ec4881ca9c17
905b7b2fa28722c98d404e93fbaadb165411d41256a0dfc806a19df0f526571c80f0":"8c5c93583dbba016531aecc1da7
b010b9559785b2e8cf660ce17022f8d86be78":"":"":"54074cf184040f57716e9eef80ed0e006cd029b99ca568fd7639c
4c1b0f7431933516830f5f87b157fdbbb2af7ab57f6faa26323f096c8e86136e49d833665a6cb3a22f7d5d38290c2e9a23
c62dea6c51b958460b263566c5c0e4be9adcb1c123b55879f405f11b3c34c24852d33c64d6563ee46cad14ce08d5919d
dbffdfaad0bef8d8ed9974f1d95917e2b108d9519b13c4f6929429d2dc44ecace7799839ffcae035904b576e71e92b0a89
f39e3b3444b75ee0705419c3b3533c793605eb6"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 256, 0) #12
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"02ef640b9f087fa48457918d7bd6e910d7379bdd89e1549118ec67880dc3
c4be3ad95397b8fc88bfced5aa76941716bf4c26696e9540d759c8c6b8603d5c40df267056c79bd8a3497b77052e4989
53493eb853b56c41f3286c09f1ec88637f95a1cb7e6e0efd3acb8a8fa4de63d10727":"38e664b930fb072112e6d47bfc5
538b0d48672a12769f3eb860243bbc1c5db75":"":"":"c399e8c39ab174fa8cabb7e73845d8d434dcebc21062edc69d02
928b0de4471517496365bbd59062a43408215f5b0f35971f4c48077623860206e0e6af8de751e6fe45eb6648a66e8ac5
e603043c5365be3015af858fa2709c6c7b1cd22701dbbf4ef27fa45e6d7f9df4e8a558517a38e26bdd82960db9a92a0dee
e98657ab514913f134cb9362756a78ae4afed3a6c89e86341a8fb20b5cdfcd56933363f83e8c55c69adbf8e8d7199bc4f9
3b72ae1c4d0939b564d98e7f052c66e1e0988ca5"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-384, 256, 0) #13
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"2f280ffe3306764839899faa89213139a40462039f4d9c55feaef6728c24cc
636819357f6ea65badc8e493b99d5af1d995d14d81e39802711977d0a1c5783bfe3c290bc469bb9af520b0faa06f230fe
6c4ba3804e39e3226f0731f09579e105d726b089d1c37c72e3faeb33768d3f20e":"e3d99860e8b1e9297c60b17904be8
525be831d71dbd3f454f085d1758ebe7160":"":"":"45400ec700a4cf8309fbea94aa4fcbdd22c859e0f7defa746085a2f4
ddb9db16efbb0c2fff798c99ff4e9e11986f4c330f3658e34a146f8d9071467228e3b0ea486cfbc81da3e739a301fe51b62

0d7d27fe9da0e4b875efe3c2bd0fde31f608015ad71cac9c95bce33e516c62fc45a9fc85a78c142416d7fbff3a83602dcce
3add6301ca6b9be565e3cf06ad6f22855d57d9c184ed7214adc1bb014a1b6dafb86989283fa3a4be10c410442d761c98
d2d3f94bb0d97ba1d5c8966eb47b0fe6ec"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 256, 0) #14
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"8f3ddc4230f8320bd18cf078c04c62e248fcc326980301174617a9e54351
c667ba4c31a4c0e7dbd7336c27c0b8a034f6fd947b0a21e580e6c2dbfbd44d01f5fb4a51dcd2199df9f1803f24c5e774f0
48815302e016aad33254d308c5457f368965c15b6204e191c2a252e4fe88dfb978":"9bfe9bc055b3215560cd28555337
2c47cca422fca574c0d22d7ce5f2dd40b084":"":"":"34f550231d31c1b3a3db331d341ada3b987120d94e431831eea67e
8d208f9cf1800549d445fc7befbdcc2488cc7f4340560d574fcd2396e9ecc9a232f1015cfb26db451623fe47ec8bacee17
56573e74e519adc62b23ce86fc191ea5e13da9c7a14496426c6c53dfa7c7ccdb67d6164dbe88cbbe7f48d4971993003ab
24f3eff18bd52c2661992e8f8da93bfdd28f01fc32edb439ad130352463084041e9871c431ba26c676ecd781299183311
3cbbe687651e93aeb22a6a44cffc7a3fb214b2"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 256, 256) #0
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"8b285ce6b4da70c83fd72aab1b4be62101bf9b29e168726ea2f670aab0dea
efc5da3404c494c6019ea33679e37cec308dab13e0cb060f66c1c83fc6fba46477d1a3c802edd7594db0b297dedb9ccbc
800c817f05658fb9b4c99938ae2140160c4a16d548634a353bc285cb38d0e93243":"723c0f287db4af285c195cebb110
4a106f22e8b243fdcd0566228ab5f227a9e3":"881a1874c800db068b5913d195058d0726458de3782ff530af1a761f96
28547f":"0c27cf271bd7931d187ec6f56038519674468fa2e7e6f994904c9f1afa346939":"51e042dd56a193908c9018c
25f1c1a8b5e2734b055c3b7fde6a8ba9ec2b959349df29295abb0a24b4715f98d31de0a369e6262c2b2cd49c5462b7ae2
84e921f5ad2ec013edc1611343c228683f4170f34a75854b1b656d226e294172d488c10a415f09dee70984b9c49e8d36
863192301d1762145e0d9e94e99bd30ce8490438ed050f418cf4ba0b07fe90a82d1ccf38578d99edf0518c4a758a199db
4d3533c4dbc55b1da19840b8f365a574aa01647819032dc0ad641388c2093ebd4ab5d99"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 256, 256) #1
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"5b5c670d3e0e97a21cfd5bc3d038f0c3d2578cf3147f5545e5118a04c4eac
727b50734939e2fd0aba704932ccaac42af316525e3fc5f1dd224131d65f8d44ff8420891c0af7c78f9cf766097fbf0f8bf
dd131db1801275c28081e6063c0c4d6242f96e40fc513608289f378bc4f18518":"4cb0e590a1d575b6a2df9cb0243895
263c894a990b6798424bea9ef199761d08":"feabcecf0648665b08a7c690add6ff75744de3916d5573145c3551780860
5beb":"fe81cf8978798311ee6d1c5d6145b3832d9ad1a1266fdac0f4fa230c631e9ba0":"62aa5e9b8a07bed2a5d3eef0c
73bbc841bb8cbf544d32a2889806ba501c6768aca98c19b83fd4fb2cabf120c05716b9eac9b77d561ffdd69682308f80fc
f1c78409f3b21749bf71abdb209660716a39c2562e8ae1b3478828bf35ec9d3f9712d95f49a36b9eaddaf1b249f023c36
d09ff1b6f3df6d10e4e336763edef9501827d5171c507eec405bae52d56fd62f90f5c58a2f1a7310530df15ca6b7841a28
71a37cae583e6b388978c118b9600840f5540af529bce0a24da8f906f601fc270f"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 256, 256) #2
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"64cf47e52f758df802c2b37a4841c73a3228738d14b439a7d02b13fa3024
715c744721e49f25a0e73e821f69786fe2d91ec1cce1d1cbf2dcbe5bdd2371c0a5df050841b6f07b1a2c0d064bc5e06ecf
2ff9904928febe0bfaf3626df5bfb79fee1474cc8dfc3ae268570df2811bc3ba3b":"c3f0b0471d5273f40e74ccd71712071

fa411b72b0f5a98c9eea9a5f7f176967e":"4df90039bbb54d8753b19ccb6250ffceb7279c05f6d69b5c47801c6fdeb1ddf8":"181d12bb126ea840bbf9e6ff5e68f8ef53f69071d223bff593a63e4e0c65ee1b":"8cec490ebe0b4837f040663de29e2c6dc801d7953cb2416d245ef66173e5d7baafbb77fd2c5ce69b4b8995bfe51f5f33cfffd9e9b1284fb8657bb7a3c26f5aac500cc7d3737fc81418c94d3db1a63f4922ca49803c04fdbc9488e21d9c4bc381c48bd9f7e5cd1ed6c6fa9e889e463dfc3a313812245a66be220266707a5358e25807ccb11f24780e5ef82c84a8803f72dbd21f55d96362d7cd8abbfd9d21f4e3dfac33326a4e538476508afd87e030d92328a91c91ffb16b054740dc3d0a2130"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 256, 256) #3
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"690a8be904c75e41342c8e2548abde2e465612a632710179ccb9c1dab76c4615bdaeda1587772638a61747738b96cfc94879325d2cf1cc0269d877eab8aa233ba8d7f1ff44e9118a128bcd8cc687eef58940343d27ba1d800aed9e2e911a8c83b8460f9d72c7b92852cc178d3d0baf6a":"5dd031fb2df56c510b3cc3c02fdcf6cf3ffa4a881e7475a8631073b3ed5e3c62":"a0a861238b2b9ea03582eb4703bc33921b5376c27004710d416ff921d6e6fc60":"3cef66f75aa682ad5430bdf0f01dd1f2c3492fcacc6f80ab351cfacc1c6b6ce0":"92b337a3364059acfcaef789ac1ae09c9ed05fdf69f5d5da7a1c9b6962d3a3c71a4041dc234f7be58fdbb728f8f5fb10404558f21d9b4c818fcadf5d6bac8bcb044e5b2fbd26ee08398dc8904c271e8d3d184bbf61f77c62fd3c8f1cc1ee2f8c4620c513f3abf5e312b431e8608b29cdf528d892ff03bc0a9cbd202b9da1d052ae2bc2dd8723198a1b3017ade2803c3dc8733ac33ddbdcef7a9948d64f72da0716b32dc6eea224bd49a7349a1c32e8e325ac11e5fad8353cf85d9eb4b72b1954"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 256, 256) #4
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"0eba7b06309f0dc4e2bfabea57e1d01a5a3e711398320925647008abf19cae194efbff93968c0a7d1c7623ee1e3987cd95c3dbd1b2ba94d0b2d416fe2f2f6faeab46646a378e931bb5daac049333129ce7e20e53117a0f68baf4c86a3ee5e787b02b53b1e0140430e77ca86f242d7f90":"69adc69e03cd113c34ae6b89c7c2fcfbe987e426da865f7c8e052da4bade343a":"729489cc7ba4f3f96f77ff365fd5380cd83cc7b17b150d327c5b7632f1cb0460":"59892fcf99ce719819774539ed4f10edb7cd35cd66969137a88ebe6336da90f9":"565e3e392a9f364df0b575d9444aac262f58ce12312d5ac9832ae6351b6aae0398e0bedd3074f57bd4e9f0e89a50d627ecfe11fe9aea09fce563eb34efd27610a3255f81f953bb3f222b15c019b9d812150f7a1f19126994c505d9ce5c948882a1f6c5cdbc7050461ccdbbb7aae597dab53a12ea6bfaa4d4710188d690fb0a0a34df7fb6bba949fd6a8565fded8e4832ff7f6b08a653a72b8b88782b8d77c1f217e8487163fdbddcc88a83d8bdad479ca75fdbcaf02250db39528456942119f1"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 256, 256) #5
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"9dea5f271193aef61bd72c76a581d65eadc8002b258a4d548c7ad1cb587a5f681e9709eab5e146833b01a79a34c352aa642a7a376595347c0203a8a0456af4e9859aea62c887166b3483e0c7acdd5b99a1b1a466dc0709cc6ba133abe29ecf3f3150d664d04baef8854fd86a5d8cab19":"895e5039eeb3ea1d197614a683c84d7780ac8724192bd6c35fe81137bc23e4bd":"9e8669a67bf80c695889a7e875a9ad1954b91e4bddd0848313b4efb4b00b14fc":"2e93a8b96ae1966e2a052db0d5c2d5b76cd7cd23494bb1170a33a9ddf39b21ce":"71a0ea8b9884e979f4ed546cee3688ebc399b41be38578f15b99d9621de0da3e671182f6da612334edb8d3a6d5e34c2872e277942854350526c3e000834bbe18cd5f2f336bcfabb42c4aaeb19b8cefa3f7066a89593960fabba244812d15c5fa7a7281067c789745127ee2b63b14237136c54864bf86ab7c377414a7933b829fc3052e8c26c698459a83b1990c093305372aa608c967bfda719e98c4c177764b72d184586f7b63a8e75f78c9e5e1dc045c3eb5b30c7147c69100c2cf910d4f3a"

HMAC_DRBG

NIST CAVS 14.3 PR True (SHA-384, 256, 256) #6
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"2b4c85aac528f5cf44e9018795a1e8f810220ce318aa174bed9db372602c0
0f68ac33625739f299241d1a8381372537bac392411a1d6849aa6610a177743afdf45cc524838fadf1b5feaaa9983ca79a
4508b5e4a275514ef4c04c233c3dbbca32a00d0a1628323b91dacbe499c1ba928":"799a4b3c9f62c2f6aa9e91604e742
dd06ff9f77b15d3799684e1dfcf029d807b":"1d15f59cb3e102d5ff47ad4c0aae13631ec4d300de4247137aec5b43e5aa4
f79":"f43801851946f97208909f1ad0f79d6577eeda70067886b270f55d626d966fbe":"f05e50192528ba1185cb96432
4141c1d195f6e26c42164052a7b7244797c3084d48bc5e6e1a27e64562cf2fa36b4de30132a082de2f927059731d084e
2042eb7720932ae8e1741f05f4c75079586924cc43a6cf3f5525e037b089674121c2741f836372f219a33bfcd910884ab
b166eeeed1840672663e0455b18bc7c9fcf20967b25dd77eb37e00d8fc40b0788c08280b0bd8878c504d982db4d3d247
6f5fe6785b1959d1bfa2762c00efe436cd217b6d01adbf7da08d23254f1be1991d200a"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 256, 256) #7
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"a716af9e058eedbe937ef79ee21cbaf4ac1ed0e2f4863eef4ca1e3e972f333
26eb6ecfa7bc9bacd3d90215a3db843b24343edf7ada9e440a206df7f38f8cbd1d38159b8511f2a93d1f0b5ace8a89c0d8
23fe001656c3dde659874df88dd60056ced293cc49d64a71ee6b23199c9b20e6":"648aa30cb2687d857d309f702f6dae
1f30edc824493d6e83a9e26d94f28948a2":"39c5a6514f3d399ac41b2640fd619312332fe053abf1b2a19472a58c28345
347":"c912a1bb84f7aeeef79d73347097e09f6b8fb7ec593176cebbbb56af866bc309":"5387674cec52da2a9743b2556f
a9874c0866e579079954cb357f17fc069c2e345c1ca80081040d620fba150c22eb1b8b2c7df082f637855c396ad6417fd
383f8e93b7bd91693408e951b7572269c0ae65be8bcc9844f9fd8401e68f6fafdce195162154b34fdd5db8559dc11cfd3
cbd3d391a45065761372f60c5182fe4cc162304061f86e666326c3332010fd388626cfa9ce1252982cae7b6eb1b8208c7
9b7b689aae9084fd180d00962fa4eea79f612ab7ec5fb51394f6f498528ad5860e7"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 256, 256) #8
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"af405b42f8a67c349bc10d4d0b97f56cce433e1d34cebcc75c2850010d20c
f74f61b23e1d2f964ad6c9a8d65c9f87749da279902d5c30fb67207d72be55451337f34aaa8e598b9ef55fd36224ebee4b
5524a93f1513fc21fa984f0a76c2bcc98ddf39823d0a87d501b3515e3ee9fd4d6":"1cbd963d49b2553a9711687bc5074
3d820588049cf097c100739f857b3928fc0":"e0d336ea552a6dbc132f194ac9ab80a34a54f4d331a55a070dde6601d6d
9084e":"91e882daaa304874fb0c063718984ac53e1f0716ca8c9210bdcdddc142c84082":"0acb19f2a65bf0e1d9f9561d
8731fe0f0c178443f00faf427973ad45f2df4f4d21a4fdecdf96c34be28e389d8caed96b515ecb215ca915b38c715015e1b
07949263fb65517ea4bcae361d76c418cd2c58d29010ea79b9420d1cedf937d3aaae7e29c2170ba88c8328664d884ace
90e88c66200033d19ffd52f668b00b0df088b7942377c1aec37b3c304521c394ec749efbb252669e0c0415b8b04b995fc
224903b0843fbaf0be1ce804c9f14a5e97afa70d0fca9cb708ad20388730aa9de020"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-384, 256, 256) #9
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"e9ecd00efafeba4fa9cbab22b1b5288c98a36ff1d6856592a288325968c31
d7d88fd2be5c82d79413b33c1dbe972859822ca2c8a92e7812479c14fa292a627a8909c3a953a2758d42f22a18682ffa2
19aa9908e06f521be8fb59ad58e5651aa9d6b95983e23e54cd57dfc82b2077bf96":"adf1f50a295d88f68e8c07a180897
d8e7b49f7cc6cb78a3b25ee10b0583a0f0b":"82de6a73568ade5e5b0d8ae37c40ff25e858a7055346020c5e47feddfef75
680":"cd0e15d764d2355ac9f1cbd5ea519ed1756a3bfaa55e3783b738c03bdb42e371":"1e592e5003fc0f3f81a7aef227
2527980cc5a9ac7286a621513b9c7ce2ea94fbfa255ef2654d673bb8cd13f3a033a7701304acbbe8d19b82a61d2e77e72
51f98b0e28e1a694f9cba2c86c7c8cb20d9c2986e52052f701596e3c837af95b166cd227f2fc00edd3ea62b57f60262712
b2f71479569c119cbce9d771f8a2cfdf832aa8d70e0a912978fb2bb33b27a185fb3a4caa3a18913aeab095ac088d14381

802117af0cc1d97c06fe9730bebbff0adf2ffac5995d299e4defb0722bd93f0799"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 256, 256) #10
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"898a6c47a5cff500ea0f5b18b5f0b4bcf7e75d6d7c92025f9920c666dbc1c5ffc48972e1d519428f8d61dfb5e300b48f2660ff53e1ffaa3950cffc50e17a874182236fbb555d35ced33302ef87b84c0ad31e87441ae365350452a39470567bc009871a3c9785bda4569af33d03d46f08":"9e16568a225b80e9011571f3b55102cf6362e26b8a60fd33680d4e6625738e5f":"b1c65d6e51ba043f63b4251ed58e9a8eebfc289f6285705f8ef44c202c9b4a22":"245ee741a2041eda22ce7053f8576c0a43eae868fd95ad7d58bb921c155b1b53":"b076210688b06ab6b57edf68126dcdfce82b6f9285ddec102ed60730aa7530863076186a3f7affbdd4ef081b7f5a32fb461bc5755ab4f860012631b74ae357fbc3cbd64f0eef8789c6c9dca894a41a005d272b4a57e761f91d221636d0ec7a49f10bb1b4264938604ff4dc7bc97eb799cea9e3e1d7a9b4bd66d88d244e22120bb311f502e66e60c5c9e42731ad320b23d6b06ae92a132b093ad924a1a7e08b5dccdc50e257bfdb63bf5705350588f61e93e4fc5042a2cad1bd6d9fbc82e875cf"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 256, 256) #11
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"8e92836dc5e4bbf9598803efb0d3871e5418cf18f379479bbcbd9262558af6cb6d97e73decb8781c30f69b61c1f5c91a5ea1f10fb1eef74b480e583710d9a6a2e57f8cfc9d0215fa73d1ce9c1562f3cc34be187940cd317b69139ab9aa58d064b6bca59ee6460c3db4e8b57fab0186f1":"6d9afc769985218745235e5af280eb45cec81a2e920c284ed5c77105489e8f4b":"711672f2ca12e7d8f32445a87163bc00f5d0f52c2f6799ba513b68c07c350de5":"426aeab2cfa56cd3146c0eb9facfbc048a504eec3273256b5e4db3d66c89560f":"56325373099fc1dd194555c3a1e69358fc7f80fe6610412cb31c14cdc70c73a74d040746c6cf388fb9718e7446888c6162de73ac097c32f8b4b00dd7f115fed1821d3786baaa1f64885cb93c75531e99171f98d3c3576337c1c41c5bfe83f94cef2adebc88c0790398d4c071488699edd599797c1f8f394b3e00e66bc4b68a7cacd209695961713c3bf2c9a5c8589d935e171f775f366217e2634ddf0db5f01ab31760ebd9ed9724292bec89db06d0145fb824a76292a35f39b01a06c43510a6"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 256, 256) #12
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"a4f1fd83e53a406163862260fb9e2ec64d4af74f5fa41ff56c07c791b6bb6abbdb203670b1849afbf0931206ad6393798ff06fba8dca3318c29d9161c0ec18ec5d7d66847b1a618bb0e4f69fa1331fd1db5d5fffdeec5a2e045c588dc95a5d5eac6d35502ebe2e6a57318f15af53e001":"39dd79397f91a97432e5124e7b9b85928f62c598ecd19626070a81a5a8ed564a":"985724541d44c8b865672759c8d36ded75c2189c2281731888a741b305eb4161":"e2dae75950e417c18f1c3e5fbd66b1cc9fa617aa695c9d03d8768b9e197fea80":"703ab1f6a5332f01fa788cf73922a9f6cf856319772eeab07b4795702562cde350a8cf9395976fd227b08134feb469ca34f675c9b6f176ad684a5b0d02b4c135a7174bf0604a1546e7d8d978ecfd8cb6ae5efce3b228dc95cb413b010732c3e7f9ef8e547a93540e5e4aaaa3b0e5a8f45b83bb11209a03883c54f41e494fcbc66c2d57c01002137567ea2f99f7a1ed6c4c6080bdaa299d18f57bb3b386278a78b2ef23a03043e850bd9fd742527c45308e5b910fc586f9f21de7022d02b1493b"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 256, 256) #13
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"f331ebcdbc0d2dfbf54758680dd49dd0bd666d0505ef6ba1c4bbfb7dee62edc34ea9063632c8e6719bbe140c3c840aabd66e7702c384700921dc1838c6c5a832c650a474e74270c378abff021d60d1a1884939bbdc51c547c72c929c0c73ca7f78668d33fba197642be8ac2d41cefde4":"ec299e456cd1985a3f1022d5c05f0ef9040cc8b8297ba5e404d92a6d36c3578f":"954f464877f7258f99acbfb9adfe4eedc89da71ca82e3581fb5bad127b20

69e7":"515f9e746c7407196610bbae963b9bc15b1658972a30e62be6f78caee1287e88":"5aa30a796d46e789c498352a
de179f0cd3336418fbeafae0d10fbf7798917672288b3b2a12267fc0435d88b4e99809c1e3067f0d65c910b12a330334b
6a23d6d30910d301438c2c999353e1f78019ba7b20eaf68b499ff1e88db0431312a66f35305c4f3c3a2750c95bbc07ccb
df1e4d123eec378b9be8894b597bcc029c664e59e2b3c23fd72841af0ddc9374ecef21885a0b54d13186dc0a66ed3c3ca
ca9e41753813ae61015a952142bd4d7ebbaa3193598be1267be937745fb0de09aa70d"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-384, 256, 256) #14
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA384:"d99ddbd82ce9937cda083e30b3da47a6e6ca08b8f59f2fc934bb3f78e748b
b28cfabddb375efc5f2025a53fd073a89b0fbec391290863ad862aa56fe6d945044e879ca05c3c019313f810dd559fa0e6
82d6b77ff7e612c7c40cd5231eece4018c5b3c0d8181ab44703f7a04c0a1c7c5e":"ebc2193d4a97b97d298f1305b2f7a5
4dab466f7c4e444831651cac29a6c5bd88":"6826aad41f8ac29e272884cb6d21300c7b0b3ca37205e1720afaf9f716f33
7ec":"5a7434648de82a3552e12aff800093776ca3e86565b29c0b3ad6c0bc3180623f":"cfc79a89a0a55dc9c6c6eccdfa
b5a9935335e806b73bab7f5eff5f9fea6aa3f47bf31f06d987a94e2bc2a4a6144ebe94d6f5aa8fcaabbf86a37c8d4122078
64322d3057b89fef358740c5962cf9e7c37072847fcaa6db693a5238ef270e8414e2b29448bbcc37dceaa75479c2ac5fee
2d6fe9ed68516f6dbd90135ddcae8a12d1c1595e0edc34ea2bf00bee7ae773c240c2bc1ed828b7ff91a676891173eec1da
beecb2184df9186c3bd833e349351481655bda91bc0f4e419fb78e426de6b39"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 0, 0) #0
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"64a8afb71975256b6196f3f93038ba8b7a4d7089f7f268134cb3f5926868e
4d104c60b44fbf3bc198f4bc58bf1260d123a5aaf8749136a86c4e5aba81692d587133d29d3b7a63fa6204ed84e93be6a
ebf50472d313ef5797d1a290a7cae086052b57e8d5a20ed22ec7702dd424d935ea":"":"":"":"4f61f6b5d46ea351dc6f8ff
55bcb915d998c8e871b5e122dd95196da241c49a1170b1fc16ffa31a6dc4f0c4068ecc6e5cc0fa6966aedf72bcb19e666b
191979f22580b6505c09a784e76f58d30af3abcbe840497ad88621a893ffe13af6aef0f8276f9540068943bb6bc51498a4
65129880df4c517f7fe70ec239c055102a78b8b0f26d36bc2634a0e61a1431850980c258326197cc80d07c3cafc49a203
16a0fa2703f850b66ce274e839d6dddba4d3e744306d768b7437ec9c54ed864c7bca4ea8d0987d815e64f685e0726eb4
223aa5eac1a0979fb335248ee59819c36c7c94dadf14474c7e2f10678da59f255474ea50c3ed5ccf86a399ba7f54ae96bff
0"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 0, 0) #1
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"e5b8dbea654b559f025c008c1f3b2eff92fe98932b0271228e3f4efa3303cd
4f112660f48057fc56ed0eebacf559cdd14f523a3e948e8037427e65dd25c1eb41560f2f78dee139b3d721ba1c278c385
5aeec3fd3a44a5331c8f54396ec3b9ba73c22da8ae1adc9748178d7d21341f7c9":"":"":"":"9bc5a8c111d4586131faef6
3689d0a7342bf601f04926f18cca7aeeb8edb129e33cae10e9e08fd44065db2aed4480b75878c6d1400d38fa2c9e836e4
a6bc1d66df571ffa1dd0a073b89580005a09d1ce81492131771ec4ff987cf8a3260c9f90fb3ec07b82ab1db526b97ae856
282ff7c62efeb2cedaacb75fda0b74df5e0e766a3573a829c32f53ef3b16ffb9d4cc1cfefc84e08aa1864f5d0fbe593abb26
b488c90e351816e2d1073bcbb599b65b196b33dab9095bb28983172f3a61c992d44345f2947e1acd2df96ccaea3f6bc4
c024a4e36868e358e5bfb9047ff11daeb34571051f0823265a15be9e4e4d64f7073bd5dc3b43ad0a4b39a5fb6bf4b154e
b"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 0, 0) #2
depends_on:MBEDTLS_SHA512_C

hmac_drbg_pr:MBEDTLS_MD_SHA512:"abe7121c768208f174ee9e545250014d031ebc647497a60e18e3462517027fea1c0e3854cfe5429bc105916e63a0d5a7585cfba737f887852f23a41039cca6e33de94901cc1aae91ac42db0ca34724b07368b1a3ab733dad24aee03bab50eaaf2acf15c2c700e5e070097132a92ae7bd":"":"":"":"7e082cce6774a3d21ff39db1ef9ed0251a6434462afd29fb8e05458b9ca7bd181a9e362ab4986c19fa1aa9bb1d00f1c3479b2b4be1512b2b5eb94b9ec0493266b6efce73d02d6acc653db9e4c194c7d169781aa78de7839e010adc7fd58efc988a5eec2feb89f2d0dc45ac6a7d4bedf11bc1294b4f312c723acbd664f28f85f676f3feb7d2d2db14b0acca2ac6d83d2877319cedbf816378365dc51368e1686f2e3cb0bd670c125cf484cca7d28cba04a25479dcfc3f80910422a583c35553ac7dd6d5a43c6cec465dd6c7ec33712c9f2289206b0f1e620ed23a335a95a1392d143fceffbc2f43a18c3426de0f2f1716f7234bdc880f61e3a1c1c2c57fe29336"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 0, 0) #3
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"07e570fa7cf079e066c5c30b6d24fd37906ab7aa07b1551be605b31f86dbc3cb3e95a0723e9344922d14185824c483bc5dc8341f10d698629736838fad6a190825a24482413b388265fb20b2a8e7c078b91090c97db01e6c6a72d1c067bedd73da1d7b1575b05870b8eee4343bc42213":"":"":"":"3cf6099489d2eaa6bc427cae2bbb4a1b121041bce2a4f8e747a3b4217910905156189420fa8b9698a8a316c537229a42509be9e75f7dbd5241de932475114fc9232c3325ee8d921aaa680078493856c2d0b14e6593bc3f36e0615143fc336054442e196dd152f53634a2fa3e74417aa2dfecf4367cbc1584cafcf583cbddf1283b73b35f9d1f1ecdb7104b80b838f2c1464ede50bca05e960efc6b62f5546a0d02e3420cb857050b49cb1e3b4ff8a936ae4aa7b1d774089c641d96a732164ee5b0cf77f2f729303c53de66e9d1b6f5eabde7fdd55bb7030671a274e3f7a41047d84f307dc1996d6efb671df8a01ca6ffef81950beab98a3e480cdda5241b6d69"

HMAC_DRBG NIST CAVS 14.3 PR True
(SHA-512, 0, 0) #4
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"99fa882ea5aa55ec9682719721a8e79d6afeec5cbb3577f1df7fe97e4edc479040efa1e51f8893210c302f2a2a3abbac2ddb3fa31758c8473a6f7c50d98e423ccf360a2f6a5d94f7ec6af04f656ad06d20e2be7e09f728b64f81d736ac3fb8263b0f7808abd5d7b0bbae1d4b3f445957":"":"":"":"5807f478399eb17159b096f7be7788769cf56beea8cf4604400f77b1035ce0b3c5d9afc256850445397d5c75d087de12f10889649d4e749ca891f30bc397b58a9b3c6321a08b89845e186e9a697377aebe36486886f74ac3bc353f033d458ba5d94634b162086b4b74563860f1f079be32789f8bfdd561e486839996db8e1de25583e2e64be914329bdbb0a42a13d668e47e4ff635d01a1daaaa29ae8459752d04b7c8ff5340fc8c97293f2b7b91c2c8e3f0519878c82a61a32687f693a64c3c1a222b664b83570ebedd96e8722ba6125f04a8ebb079597394de9de36ca42d828f90c7a5fc74d1ab03be73f7c5ffd332b90517aa6ef8c19aefed182de688cf5f"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-512, 0, 0) #5
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"75336fb0006f7aad995ae01b3f3ec24cef46d3f7ad07798e52f609ec34b266f1cb51865817281103b3be2c2bece85487e979f3a31ba75d6e6e4b357811b4aaf5fc958406721693eeec21e8c9808ceefbd17a0a6d5664162e7b988c19dbc911b6e3b68e90a1e6a3c9c5a4662d954ef5c5":"":"":"":"7e13788c362ebb6e6ae794ec50d39c2cf2bd25d8769ee91df5d210b3bae5021801e0d59ee503ea177dc01b3c606daf67a2fc8afa9f06b2d03759e2191d6dd0e916b5d21125322bbe9802259366a43d64f94c5408e62709d806970a83dffc4d78ff86dbcc7540f34dbf026dd308ee28971ee5e88681b342d15dbbbaff92a51e4b40e4c50e0b1e48d153d5d6e950de8a37326ddaf504382e20ffa85bcc91fb3f7f56130ad67250c7a9f1ee5f76cb265d567d448c50eec4f35c222331bf2dba2b00cc660e7015fc1e6a7161a01ccce02b5800cc1516c330e76f33789fb47ee8e13870ed588d145c016c3f73c6b64892b4faa7dea4fe536c5349fdd171019442680c"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 0, 0) #6
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"f6d7401663547661563e5b2da208f1f8a4a0c17b97ddf0d4a4c1a17c23ee8c7d00d037839f2d95dde6a96886cd67c9a92fb7fbf77ca088d1e46f2dc386e16fb6f1d178f7c1a3dfe202f05d52ca20fe29b8084a9d597fd6b0e53f41a13fcefbb8aa5d539c7b09d8e7b8f687b3df92c606":"":"":"":"4fe6aabcc40e158316e49160ac523c41d4df8cb041e11549dec0a40cc854fe4b160fe38a1cc22b779789ef07012735f457fcd2a5594b344783cf6661d83b046cc403b1feb96cf81b05038dfdb40d2a027ea4ba93caf77f53fdcabc361ce48abba784fd9feb722c477cb9d9651d9db6d088e097a93e1dbaa2c3db1503d65680bd4b47352b04387f9c15a1c3a434e93ecc39647dad810ed96997f107e5131101ce20d4be82cc67d05309373792e15e2974aaa9aa9bc9e681815e07111f1f980fc8ca882478c32fcc3765b8e422a5369dbf36f72390ac8d3b728b8e5deb3d48e9ea85a31a0432b813471e6b02e4a12ed1aee0ab9dbb3c3e66217c45a174f9b4ed3e"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 0, 0) #7
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"98bd225cfaa81e2111f83b4b3b2dfdf3507fe18aa97100062bcb5a1f665c091002fba3d84e3886048f67bc7f06750a19a65503d83a48045cd9b128c56c3e474b7d658fc590348bd9c14013fd20d2df32dbe9f9b73d47e43e58a6ecb5f85f93b3546817134746016f6886f6b63be830e1":"":"":"":"05cddb6391c5c2de3db999426f31238b5d3e14a35623272d6a72c73947b3521017cef377415dcdf09ededc0d34d9880b9c44f28099f270844e58f9a97f7388df83717ad48972036968e63f281fc0abe53135867cace0e427ccab04e0dfa8108d87a0b7cf7be14ab50e59e4aec8d367f54805c534a9ffa2f3686712caaead514caa30b1ca06c668b5f271ad8fd84909ef122d2fabde7b524d42b925a068d0bb265cbd7c6505a4c2c0bff7d47068b76f350fc85c745d099c78bc73f9ea0796381903e0d3512283b7fad05850e1bdf63b9cd52eebfed270f1622f057f102d6ab19c63ed59cf2cc1e5876257ab03e20e62f3a77761da32a5e1c2f8c95bcc7534ee00"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 0, 0) #8
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"7a324a646b53f28808f7c44303221ab36324d1c97660f7c333b3baa7537d1e1ea038b8ca6c159d91d02f3b206eb927570aac85674b59f419af2660cca8eb0ef996bac65dc33c08a946fb2abb9348dd7ebce4c71cb9de11b8d59aceaee2c9a29b154633df643f3787c2672ea7e789a2b6":"":"":"":"3c09f50bdc35e0ee8bc033da716f68fb71a68a339e26711e63f564723a70a0b9b4b01ae5422c8ce7cea7be0b35f6bbcbea110afc9c448d85e7a87d43c54ce117dba86d4b95a754c77a4c8ef5fbc11c2525173aef82f11f482611c426887643da6daf51bb3bc462bd5efc68b4b5e7e07c7cd991a2fd8672a8a5d8490a451d8df92057df0bbb8a6063489b84bbb0a75813ffcd498b146f11c5f16580dffd38812e305caf60d133679c2b8c9564aba044ae0192a9a5789c99cf5ec40a3c775d5976391d6adf9e4c77ecb0a8f3169bb3cb7e5f2112e18c44fb7505e7d5c4e6c0f425e8e552f75a340923a3186e49d7df1a3dca3df907115c075d39844548dcbc7655"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 0, 0) #9
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"59b84cf5a29b45a3f8e0ac384bed20d970f2b6d89661bbe2af90ef073eb061cbf323a13d0643dcdba902df168ded7b6094e18381181d91d3734cfb4e44cd4462de81aae064a9ae9d156bbb14079b78e2f612c2e0965d15b2563d888e2034d06e55f939ac2345c2638443f83b59152696":"":"":"":"88ceb600d0c319c5f22e4e91c5a1319fbc752ae314868f1fbc6a4d1c0aa4b5c7054d64924f841d06392294866ce399d9fa2475a4f53f42853b68f9851db002655dc96cc799fd6ee1d4498f005e25f76efb4c0478957de4b26deb3102c602fa08179c8ef26ee29e9c9e896c122e02650dcaf622fff729825aa87026ed8dfa96e9fb1510d9be44123dca5b9521ef9500f6e3832a7897a5e513e971f1872

6d32848a6452ff7347d5d8df6d401eca2b83c71a1d806a5374bf6e6a98013beecdeeba9b637f23808ebd39fc726061ad3ce44b02f73b2e6e7c558b74bd4a085c445100c627f2b71c54e5a43b7d36c131274c04a0941fd8cb584dff445037f622f4d69c5"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 0, 0) #10
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"64688640a1d3f610528eabe2948e2eab2b453a8cbbccf58bb02a72b1bb466b8277f2c2f829fec66872cc8d6c03280b5074136e7f3e123d6fb72786fc29d1b55782b7283285cb53c4185801d2d7333b8ce76c1c661c1ef65864b8dddce781f5db520c666fe07fcbe4bd5ccacc115fbbdb":"":"":"":"a7dea45bfca9c6fe4ce5650369eee402b747034ce93272ffc44eb715e49e6fff83ce884956ed4eac3c76b5e664403040cce0d5343916a93bbc16933fb451432f14891473c93be2e17813f8119f579bf7207348020b2aeb7cf725a186db21fa9c16c27d63ae28b5d5299f163ce8d28739a1d583579a1c462f0f73ab2b6b0eba5b493c2dbc7d9d6e0819d80868a6b001971e8c205cc3b472ab62cbed1e3a1a0c0a6f95c5694f513654d7a240bb6672eabb745bc60024cdfcd8179fd3d5300b878ec93df4da38e00fd66809bcd8f9be8384cb16aead77de833e90c034ce24b18b096a84bf0281e0462e9e3a43497514b8eb283edde2108d425839aadc9e68ea4728"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 0, 0) #11
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"d77985d85e130fa02ee13b55cc7372c23565a56f588c70154b7d81dbfb8ef66ee861c781fa258019ef91d101367726ca46a60c705e0e3a305ab6a7c5179e6a14c6e7de93e5c95956660ba7357003f08a25a42e9bfc38fc882a063586285eebead74a78296c7c3e8112062d7fe1adb232":"":"":"":"94307b991cc83f919caee64c25db23bd3f456585b6edbd6c8256cbd9d12b8430d0f3be857d42f1437228be13ad5013e4539bef591a818c5efc7644da270857f61373008c614a06a6fd5fb5895f08d5ac4c84b5060498af63459629ad038d2f436cb5efbf258f9d2f1e491ec6d0bc0450c092939b56a489a89649c1ea700fadfcd9c36b8854320013de6c569234f8ca0ab171b25ae93048fe77e72a0730f6b3edc2fe103c82b78698c497db534000db2410c7945cb36da5a451834abd5035b0d4a6938116eb46014368aab7582352e2788691ade1dd337d7610cbc327f3664415c870a022f75d290c83d917c212ae517339d596c3a1cc4a1cc83cc7a1bd94d6b7"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-512, 0, 0) #12
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"ad321095c835f2c49f3abdd0f9117cf8ea30b237dc3f1eff7728fa9b08d4c0fc073c82bfae1b5771728917ae78d5e22f4989019b13c5f04a420f134d1cfcf1be81408a143e1372a468c1303292f717daf4f18ccdcb81d8c7ac6562deb4e07a9e146900123f39ef49a91e30e22cdca22c":"":"":"":"be680715dc989f5f1c459695603b2b97644dfe17f305beadf7cd3ff23a523aa61f3074f5c533cf8e88ce74888f95cc5e463de4ccec3aea10498efc0c335692fa648a1d7eb774037b993f7622a43f9fc4c75ef3d1a473c18216746dc7341dc9d78e7431291467af9a8c95d86ff407335226601541da1fc1220b5385d18833f792ee13f11641e2efb56237ae9b7ab9c1a87aa03a442f06cd7a18d8518a029e36e85369c2b52e351d3b435579938a05fee87c44496c4ff044f267f31e6d80f149d54cbbef4cfe5f249a6724c53f0a2082865eec01cb78ddb07667b40ec7391ca77fb48247b31b6dbc15fdefabaa6cc97d0bf8ebd34ef75cc48d5ac47899c89800e1"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 0, 0) #13
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"67569721ff02c3862cefa68283ecb5b9afbfeb8395ae944c55e5da1b21b6c2270f0100b2cf014cef7a2e85dbf2738e97f8ee97eca692130d6541fa900eeef6b9858497faa2cd47c6874590190da6d5fbd36d2a1e124a94311c8508b9f70f34b97c32df3947aa4a0bf197b1ab35172233":"":"":"":"8543aa086777415188ef995fd4bf5ce52776c6574b7b769aa61d1e83a4c3ac4483bf90b492341443d6c92e14fe7114558d1855826e41772eefd5435

2a38da94293e317e0a05345a567e30e2299aeddc4980b3e797b7c980b822ff625db3ffed1f0acc314c11e2b62972750b0
f448cbeeb08b7dcff21761b17fb63fd1655efadbdd6793e27c47588638c03348ad0fbc8b7772b7f7882b66b9cf4947c934
43f793de5c2a4131dcbfe982ed2787a5cb0d99ae001707d12cadf5059eb4f373e7b5e4a99a28ff18841f9edaed7558ac0d
062589cb3ccecaad4d9d6dc1a7dbcb35aef7a1738c6c66ba04e08f693d28f7499f57bd8b02d97eb3fb36d8bd767eeee07
096"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 0, 0) #14
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"b19d6916dd39eab11165ff2066fea53f72488a78eba473a0e141de1d5b13f
ecd79e678b4b108c65f9c38fb2a2e5c29c4ea9dd450593b6b3c7be76ed2cf8baa1b44794ebef1c1105a445b79aafe471d
9f9881be7e81282bec46431b505ca8bc5049da52cd4cb075cc818bb79697b739e0":"":"":"":"abf29caa9bcae107ac382
204baa2f46ca2742090a3c895e41b345a6cda8660e44000984173f57e79cc7ab869d8d9f7f2d855b171c3007ff9c82f2a
5291d509b6584f04346361de9aa373f587b6ce8cc43d589d876c95e813890c26ceae61bbe0b88072cacd0b857d6b33ad
9e562c8e1aa1592ff16cf683e81142caf493896fdb325eef5ab6ef3238cc3eb3baea05825e57533ad8cb707b373d2d0a2c
048a07bb40a5a68d14d21a796fa97db06331b480bdc39701bf2298fd3405a42f5f6b76b9f40dc8671db632c588ba8921
0767bc165ce88accc78424216e357cef52a31e7601d3f1cce1b5b5d71c3d622c9f68092f66787b32d241716996b23923
76c48909"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 0, 256) #0
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"73afadfdf46ac9c528059ec5e4f940f120c19beda8d5b12ae692c1d3b1252
6754ce532c291c8ce823aeaf923b3be8c438d8b2a82162bce020237440d3445d4ef91793b983202b0f8532be2d78c344
69d2c67fea05495feec67b76615967efa6f6bcde5bcf18285dd3d8f9b97b3463813":"":"7172619bf78c088c4f0d5b358f
63cbcc019620c6ea9ffa31e040ec0d51665989":"a0670a6df2033cb19b082a3c83fd2eecddd9b9caebf3aed0b781ae9d4
ac8bbe2":"38ebc242f240569f792379afe393a76698fd07dc05d5c86d00791c1b9d1d79f180c4360fc8f2e5332a961198
d7486750671e14d39a2b4852aede2ae9745484ca05d7421191571d334cd714b9433ba026a058cab5619208f2e54f2d4
8286e49bd0b528d05785beb4ff8953fe875cd2c92277494f2e315ab2790a1cd58f02224387470bd7edb3181d2b587e5c
319a262c7806f8b75e59f2857871d8a182ba0366cd3a968023c22582ec7bad2a204de0eba3d24566f213c1d88ca2b2ca
8cafd8149193949da885bd744323f31b39956fdea7bccb1d64d3f14afd03e1755962d9df1f2507098455584358e951f7ff
8619f1aab96e1481ede5289224053f603a98ae6"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 0, 256) #1
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"cd453c328ae68152e074e18b660f03668cf264eaa4109afb941816f7bf1f7
3cd4043d4692942472482f44e7d6ba5486dbeea1cf1de6ba6ea1606cac41a92e34839fb26b5a9bee5f4f475558a5d8f67
3d838247ab81aaeeb2a72be405c3d24a625df7476b1133b56f6e7aeb184f73eafb":"":"c6c23cdded140a30079f35cf9e
2dda6bb2b277d8a212d2fca1a83b507808e79":"edb8c8657883a17093ffd355e8145e26f65ce7071ba38c89fc0310409
96a9705":"635a7dbb7ff1dc4a90ce91ba13d79e09819ec7387c277c91946b59fad4bf5d606fa75cf03b6904c60f9a7069
7e662aeeebc7ba2e6e94632c4c5f3e1686e6e9497945c8889243719ad066847dc11efac141e58ac29d6d2779f702cd1d5
fd0d82d232a004dfdc13c09147a77d71774761ab4e760a9d2714e9ffc52402633c8c3020b7b9822b177976f21b7e98cc
cea4a7eebe1cf9a604bdfa36f19e44cf4308172258576c3615cc26418e86a7269e0f88af7f15a114c5b8c6f96b8be09857
2aec4129fac371736b2fa0a88f1b5480c7c8657dd515417edbcd902b3d3e9f7e10df45160a37284933dac5fb105da145ff
13f677d99c494e279b0b1990234fb8ed9d3"

HMAC_DRBG

NIST CAVS 14.3 PR True (SHA-512, 0, 256) #2
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"3c4fed3a265818f6a323b9d52c04a92698223f3136c77428b29e1cd6fddc7e4da48d9115c5ad18a4182df480eddd529f35e2bd1908dfd05964cc3fefe53c38615f04ca5e12c06872a695971f9144f6b97bd32c620083a379d4f56e820105c5f5b0f98539936d05d57f6afdc191cce7f4":"":"7271afbed1b1f2be5643c5bdf0b6218247a6128bfbe2ff4d745a926a3f35d0fe":"00022d8acec09266a84673d056e7b235f0608d15989ddfd7059647522cf3c3e4":"610901399f45ef5a1b747c57b73706509f569e3a2dc84c6603f403cd49e99e288c9ab77d00e974eea625435dd126e9e783566a71396b1bf6364b36305d1986157eb59fd231b6aae35190347e1560f91bb388823504e563cd69f84535559a446ef83ae625cbd1c5a4d114ff394d407f19c8f9f906290dcd03a7b47091ad07f3b190b83de5787dff47cc54a3d53dd31f756eb5de9f7c965d70176a8ee71fe869e960ad33cc492e9568e5748f9ca869ff143252f4c9ec8a0bf937f138f7ad268abeed27e1d80bed0cb7b74411989b313043b1c65c8847cc3dd6d48509852d33903253ceb074dbc3d124749d8a8e41d27f96f7fbc9908d4ecbf04f60187f1a42c33c"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 0, 256) #3
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"229b3318cb25189e12ce9ef25acd08bf56c631c6058daae6f377d58f7574576a4c0b7c634e11da5ccc02be824e6effb8ebc0d5403d79bb30572be47a5ef88fe35a0421dcf9547437cd3a563b6be7a158a7f601f75347509a12dba8d7f2abc7afdf89c43fc5538318654fbc90c3f51c5a":"":"f8f98c65ba1f619d376d41d1dd480d4a0446de56e0b3dd007ef7e1cc2bb98def":"b3bed7c4c2e1a762209b1fd2ce9ddda8fe47eb70225e60d5c5887a61bdef0009":"2467978b293afe33a96a7291286eeae2b1c8b5753ed4d45b3d5be906cf30a6051095cbca79d2871334e049b729068924a036ea914a5244fc71005385ed6ad7c7cdaabc267a8ef0074b14189763b5de2115d30da70eb815262aa511e9859b9d1cf2810c910bce18d179a0308fed6f6f911cde79031ead39f499ef85f7525140f1c497fabd879ae130f73fbbfe8c3fa749df48e484cc2fc313d234b5d0b4969098842161120605 9b42f6d72b0e5fde6bc11291b8533a9aa2c521e54749bc1929b71ff05dfc8f1716c9fb13cdad16b35d194a48ae377625300df479d3facd20c3b8fdf18b88b57753065e542f147248064278611e99ab92b33c68aabc4da08a49bf"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 0, 256) #4
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"4cfbfda3fe8ae7ffdd8450a52c78388a6c9d93c6e3ab537c91dffe23b5693158b7919e875d9ed6827a33d5ec5bdcf061c311aee36953d13c16f0e50f455705a9ab7a436b039551187a0f42e5f90b40cbd44e98cd5295550cc46e33be6f073a9e6c02ace6b0f896f9ec56ab7e8be7a07b":"":"9d155d6754ddcebaa3dd28ba27946ce3e22de29dc1db8359378390295e5aa287":"ec634fc86bfb45f49a1197a70875d7addeb257f1245375aa1f01b3bc359ed73b":"46f5a6402ea9e8a008925c8f5540c4366c599166baae8ac762da101550352f35ed9d34f82e7e2ce042cd3569be557e02aa87163d1e453904c5fcc998fa64c8e18fde61a8e54c21ad4da060943aa79de14317276414e71a8c132053c4dd35da0da1fbf7f0cffd264d887c8ae4f358afe7e8a1bec60fe7b4696a6b1c00fbb46012937b715ba8eb173e09c1316cc361819b24f7284f983b6824c39eddf3d0ba58e82a2c603d854cadc41d5b12af0a67b367f411c5c91820e414e30b3d2cfde6876a3d144a900eb2dcfcb750bdcf09c0a01db79aabf53e7f045b9c824c8662283bd4376c7179096c5c9c784d6c3b998c4d11b7ebc01a4a562852b9b82bd313fae0aa"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 0, 256) #5
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"3351a083c1f6033be5cc879eaf34e25542ebabb2671b65f726e76ed711ae073e9bd7ef6d7888d6fc31e51dc7f60e8b07cc6fe94ea0f22cea1ad54ffad09700596f6320d980488ad48527f4e00937b6f736ebf1b9166e20c5b812c8b85a2a29d91ebb021b19d2374ed4e2895d1518e6cf":"":"9497a1c85796846de8d8b70d66d369ef59bd91203660d6df2935000e8bfcfe71":"8a681d6cbe1cda5e0f9eeaed12fdac75b7bb33d28d6855d498b6c61cd

7ebca57":"5148fcd7c01eed1da1d8f68a706268b5028e4f3435ac5bcef9231cc81c6b6823156ff7432e51651d0d02d92e
22297dfd12a9d507dd3137ca8ef216f969ab67f54c8d5fd5c22c9154b6caba4a147ce4aa20647e2bcdacb727cb0810e41
06494db0e25e7e6f939d29129b0c5cf47adb35629006e6f5c7c1946c1e647d9aecac7fcc488a1c868378e014fc68afb684
e1e043f53fda4431ff031107cc23833975bdac060783f9cdbe96ca164ed75c3280ff355e25e165eb36cdd4d651cdbec053
a38b6406c26ab6f16cd0ffe1e8e5a017e25c5c93fc7ba11385164337d54123ba03e65c261e8379f2ab24aa0d27f57b9d7
e0fa825f06986a4fb9b9973adb87914cc6"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 0, 256) #6
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"3439b57a2d19db8b7e10ff9a34ac1d29b8d789b05f4cd2bcb0376c6e184c
fdc695c6e26a0b15b11a685438f48dbd7433d63119fffb5e317d97a5b3e23fa6228221caadd163b66e36e41d1df89473a
d3a114d25c8093128e2219a7f2206621b99ebe673bbcaa9a369aad3339927773b57":""":"dd1602f833057b77a8c763ec
5aa302326920bc2dda46b4b83b3600673c1f4627":"e2328a109a4546f4311bbe3decb53b3a1028984ae73ef8849bf682
ec29c9b5af":"e02326b477271366128cff2c88b703814c52547936ba90e776e383620eaa6f2a0aae1cbc6bf9fe8c395c0
88edf27ed3a3ee6f242dd6a6c3deeb19fbd7ab3e7d26b8c6f42f86803b885c733aafbd1c59e77e43277e244c0e9afb0629
af510d03f6eb547bb0d455163d14beca53afb4e756b82ab5610502c1d74406222142f1cc1a41b4188d7994397a7ee719
5482f22cfd997a611816e331cc62387c8d28177ea6727fc773c16278194b419f7e99fff2593bb0e6644ad653b63de83b2
44fcf531eb6db5716e60dc260510920754504146e4c727aa29b5659aa97a3ec63d07f9387277d487e4b855a6ec053289
af6e17284a6deaefbd526dc3a379e5ef4434c698"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 0, 256) #7
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"f7c4995379079e036b9b10db6f163db23bce7399fa8b6268099fa5f2795b
67ef06ec674197c73fe47eaf0c4986dd3566055eb14934bc8d5272baa751267c1dab1d52da6204ace6c869bef56eac006
abe8eed565693e1854619266d400cd3f70222b6c671120173fe918d229d5e566886":""":"23ec7d6ba9a666ab49df45eea
c006ad1f4f0e2aa4da2061d0429b510ea43d93d":"299253ffb0481d2a1dc2ccfa666123a3bda652666a77b52a32e4cf92
a65f0d61":"4e4573833f4ee5dcfc4fb057e3ff8a7cd621b1c7a51fa4db8d02e6b62462ea9ab62414cfc3262569192a5960
f8c3ab164ef2974ee03815281159ee50272730881d997a28ea2f9bbb2d7f2eea719416b80c73598e524f5fd9b41d17f38
6a30c194e2788278a61fe3f5633395e28a8f142e897d3b6cf34c00fc84a4407e0816518b218eb08a9d161981c84bfd3e4
7f3ba36f54587d62060e0fca65324a332a9aba7cc1d0e842bdbcc8b1bc57432f9d70e6475959da2fff2590438bd7b4faf1
9ebbaab175655189050781b7c7a27e9867073e1efe45b47ba3f86414229f5d2cc08a1d801f731c3099b747c68c1e6ca86
3a82265d3b2819cb0d2d4e80078ee7584e5"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 0, 256) #8
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"376829aa929aa4fcad37b41f3a23bec28386329ca689317c49bdc2beccd5
066b92e763dbe8a80fa1a1d21c38130fd999df05446bbf128bf23834d8c7cf89ceb5ee6b21124eb6d4966f0f5cdfa59ef5
8592dd2deda2f611b6c1ac8ea1b1dfb3a51dc5760c3a7e82fee6f09cc2b7a74d7a":""":"f14c07e0ca886373c563ca544c3
ed069de697c538afaf009bbfbd935995955f6":"4d71578fb5a3211d3bdda82396507fe5193d21a2f70e6c2b03828fff53f
5f6a4":"f6df98f9c4f7dc64208aa5804be843ae9a989bab73f6a36b603d1549ba0a58cb6511bf5776a786141e48305856
b1db6f641975d0cb5102b51b539496438cf4cb905738c919e1b06092f1af89382fcab4e365688adddf02fc7ff640e111d
5f3bb2c06da91a77242e1055c0b56f17abe0807b18f6a93f613899d37762bab607c05467dc89e58b21ac50bc01fa52d1e
649bf74841b9643adb4699ec6ec0bb4d297c138fcec1f4249b9f9ab60c2743ab18ea5e202114260edff93f4148ca772f94
572398bb387b78ccf50d6200f7369bdec44ba6403ae363f3b710d464b6f9389359030b61b2b6261addf488483e0c5e4c
f854d9b601a1b1aada803af8feeca913df"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 0, 256) #9
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"981da820fa53e7184a1a214a114a943953eedb39e5bf2c3aa7028aafe57e4
82bf4c0dbdf862d55afbd0f0a97f6c61204711b46a8f5d1a69089add789f39cc3d6dc7fd19af6a630f03b1496d84aa83f1
eb24c0d354407fa9664ee5f4c8de4ea75f05a17621aa9dc58ef38cdb9184d24b1":"":"2f4d6b4724cb715b0d553ae1ca6f
3055d7c398c1c031a3a69946f099116d13f6":"76c1d679786f1752bcde1108b9977311f4af9e3d5f5fb9eb52565d0eff9
0b4f0":"a5b531a51e8118f33b20edc76adcc36fb0ba8e7f752518b84ce712479ce749ea893fd31368b10dd6832f9f2bdb
ae488dd9668a80c8091dde61e58336a8160fd7a167aae7a1d0f0af077f600b5ea21e64847901ba658fe40f20083907b25
b30cad314cbd3f194f8be407359b94be74b34e2b4e2ce7371c12c28c7c7bf0032c03371a6247b60a113d56cf938d1e4ee
f85785fea90ed45a1b50fa40228fb23f154175fb0d436ad726306659e2e9b6a816e9f0716781a774b2c3386812e872fea
9192fd9fe148bfd7a987f74d1c7e7b60a00bde3e4ab53d3fba5df0e2cb7a3cc6bd462e43b93871b3e238634174322a880
78cf386fb210aa4df2c69ced8a4f72b2d1"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 0, 256) #10
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"909f30f7186bfbae0615a701e3fc362fc6e8ce42162cd16fed11ecff70760d
7d0679e0b79fec33f83bd722f2bca339e791e5db7af16fa629c84d1f4778d1b1dc24c9813711507349c26319e18084755
cc392c9c2f2241406ebef3985a4ccb46b2d7c5f8b79321163bdfc3b5e21eadc89":"":"1fcffb9b047f2e904899eb6aa815b
2eb51ed696db2478118c4225b7b308ce069":"becf0c41d3930f152260e0e6f06355bd0c1701b81e699fff7d8e5a750d5
7b980":"405cb18185e295e35bb8f758b0392d8e323555529b84e1dd0823586dc35f25e27c5a26da87ca57b1544d04b9
4cca967df7d7d89e00d3c919960e486e6f4cec6eac1951064efb3311e4be348558bb693438753460c65ace14479fcc449
15dc6b223900fc84add04c48c57b2e9aa13c69a2cf2b0bdd2b2cc70c49a32e5fa0606fb1523b1da894dd7f6973050471a
726fab3ba99de3033ea5a0c21e687a5ec9d66ca8460d74e5b1b99143ddfd4af6d95f6683b103133caae77649f00652f1e
78295134ee42cf35bceb7d52f6cacb41effbb2ed661d8f89bab51a90c70862ee5fd5d3c6060ba0b5a5897f796f4107efb0
8e5d82501692401732abf5237e0585c9483"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 0, 256) #11
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"9586ebe27de089218433143fadc74eec6ef7c8d077536f7ecb62d412ef0e1
63437f6d84e8bc6e97ec02097815a99c338c8f3434b286ef26b1c234ebf1bb1d216b14b4c3b3df48ac3283b3ec9e50c91
24a717eb398941ec0801f95ba6108bd9f89d9fbd72d6248ae50961354280d92df3":"":"65d08da7a1fc390f2400efb575
20e16da932bbd328a236163c40a540de585488":"a1ffc217e71d1f1047a9657d61ffad559da3ebb75d5af74f3a1ca9fc5b
964f76":"0e2958169b413044917124f867d8fd4b865587505d4a18040012319dbd472688bd90a28706c56bd1549271
b1237a5cbff1844b8e1947ab97d0b1d33bec5ea32ba3bbb5b0986d95b8aebfeaa80b0a132ccefe9013cee4fe84597cd2c3
deec46e5c4419ce2060433cfb696e34c6f3d6298f501a56dfd85ab8a9ae8163e5d09c707cd69a3db0a1ef4a1cbd9a7539
6f7face5eae9d63875898107e3043cdff7f6a7fed48362792b7a43771f06d97085525f5f38aaf38d5b668dbf84276c2580
29cea7435aa107334e69ecd50ddddfc8cf592373fdd7cc28eb73e9fd2d2d541d0d88f9fa1bb62ede17667f4c32cc9ae203
8fb7763b922c34d70d5805d3896bf8319cd"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 0, 256) #12
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"90b824b7aa16b4954d99c3fded669a83d67460ca2fa861468f0ff6e8ef61a
ac7eff878ac34c2bc59a14dac9659cb558b11989f8e34d1f27c68ccd71f45f7a848c94ced0b18c175c7e1eb50fe0204cf63

0e39ba3deddeae5de4f2c3d254d6d9a747f486e20106f5a6d7b05a67fe474e57":"":"a76ba2ac232a282b3829d9442587f
cff4693350232e976439b5b9dcbc1b704c9":"06eada44600f5d5eeac046e16cf576d59c1bbe6c608d7684453f353a644c
d031":"c6d51f9aa217655be89a7b85241dac0cf4f59d983303c3c5e7c279cedf298072fa1cd70a2180c3b3a58f553d6d7
dfdd01f995401993ed6f2cc3778f780262f93755c9f8d54d94e702dd6df82a737d57cb5784f035e7b2983e6253d0b2c26
e4dc7182d5d06628bf7ff8be110f28b274bf2b9cdbc14d16fa1c9f2fa020b0470bb7744d04332c23bb198d2d7f98f15fda
b1ae8bf310dc3b90d132d722ab183f806cdb324c503898f91d9ce12f8dd1942867b1a169089cf24f1508079db6184ab4f
bc80292c439f7fc2230c22bcf022aa8ef29f23fd3cb8eff8fd9f033b5620d5845d4ec5d0c8f5d4f7d02dcd2e9feb143fa628
85bf140aacc7a3160508ebae8183b"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 0, 256) #13
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"0ad0edb50bccfc0fb68b5e7b5edf8ca338e5457cfe44af3fb5d683db120c6a
09b9907dccf135c5cd0a97200abe245e144fa70365cdb06dddd7b59a557831ec9c3ac14b3de791421cbaacc609bb7659
c4e178a7158d7651369655f9c570674fee2c5aed961f3c6baa0a092363b388add5":"":"f9880c0023486c8c8dcac2b401
00a6e2bd78b9289e20a72f4cbf46fc156619f6":"f5bf191309d298ce4a39daa668d8c99935df9ae31f5bd1fbe77a368285
8d5c0c":"febefa9a23eb4f236d1321d9abedbe0bda5de6fb8ae4259512dbe3f4df7e006e571d8b55db6a438de63917a2e
476435ede5af77630241e7a213005f205d3857348b8282e790972e4a5983009e052cbc6bfd00c08306d346c351f32a7c
01e5142cc65d5e951fd9186a098f6f22a5e4d5abd80982d1da86c39b1529e36d2341e18859518a425cbc198e9dba8955
91a1ae395b148f033e1375903fdcb478e8438e0622544d6cd990e5a4633698dee50a623a2b7d8596ccd647db9be1c2e6
f383e5316081f2c076dcc98483279e87594ddca5ec4ef4f9f52439571f671087bba02708af107b771cf59bdd38f4f5b6c3
6aae8112f85a9b2828e048988bcec68098660"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 0, 256) #14
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"0425754d1610c14f6be928608ea3ce731ae818b200c54341aeb178f69e14
5fc6bd38473928da0d3638b0625d06f6b94fa009d920238b591c97ef48bdac9021fd85f19ce809a9627183e3b621036fd
7e3bfe1dcf51b07ad45ea924e2d933f15c1172432b359ad72149e51e86e56ba7768":"":"f746e854338d81d89e81ba365
5eac565866b56b2faccdc50a36156fe2faa661b":"06e81c2ff61b7c7e51f5238babc38887bc10d5fecd86b7a6d7c48baf4
aa5adcf":"cf9bdaaa8be06039de98833ca92947aee84ab5a43b71a90855b2bcde9b6e69255a5a5e24c1bc8ade2b6338ba
bac8fc0b90674bb700080951425ce67c51636f35025171f584f62ca49933f11883c9fec666305d88ad2d359ac2e0f2472
e368332da2f5a15f857c8e8bc7b4897f7e12187ad9395a47a9f271541537ae1bb217f88f9b689933e5c6fcbbc2c39f5924
862a4a68e068d06a485f2d80583eb6606f177f9ca7618e0ec018596e0b98376c95fc159fd68aff1a0ef3514529d4a717b8
efb7b4764d11c0619ffb0b20106a5a541cfd4e68c002b99bae85f0e99627c91b3dc7f27c2415f7ceed21c542af170bb139
8338041c181da40dc95bb0deec6decb48"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 256, 0) #0
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"d7d2a9a0b97f4564e05de6db7bf170d2a726e0f5eb2970839c4a0c686ef37
2faaa5d8afc07d7e9a44904fe9f7359d8b6205c7ce06021f5dd60656247503694960c78aa5e3b3f5008d48c6a264bb94e
1c2950f734611e3e10291cdc0199ab9000a9c2eb74081b3c2cb4461ad6406a38e7":"db994880895242ced06eb291577
56b25052257bd49ca08c7208d51e7b0ddeeb7":"":"":"6a45639360130d0a679f9addcbf6f46b9945b3b1e5a72eb17514
4e62786dbcbc8073cc2be8cac421b9576ec496452ecc1a611b1e5ac41500c4213404a2311247c5e828738a8cb55f67b9
7f39d05e36eb29871e3d709f3bc7c72567e776ae736b63c06f5b57c1127e305387b115f117e302727d042c2c0979b70e
2a0674ace2922bcc2839c1a75044f740790b62b078bc3cb056a34a9ad7271e02a1fa86ec85226ecbb9b126c4a9b3b0b0f
4ac6915c641af28b34d7b7da6bbf4ce280671c52eb919100e198a3feed6b4fd48c01d836c363904d640e475e0d0e6c6ce

5f25d0b174c561ecbbae201bac53d8499706d83da43c268bc2c57e2405ed016d6198964c60"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 256, 0) #1
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"82037584f80266988ef6d15fa6003478c20d33265530c1767e3c23f0a0a95d61c9262c26dbd37083066bacce5f93dc86e2cb95521fa6dcc9e4d01c469c4a3fee33579c21058975dd91f9043d5ddb154f5390c4ca2c813938a8270b954a7c7197ec382f02c50dd19598017d2abd1e45ec":"52a6cc9fe891945e5039e95271ccc44ba9ab57f62086837ee64409d0fcaf1973":"":"":"c60f3bca5d6b1130c6fba93e3da9b81dd763828caa5ce81fa528e1326b675585bcec1b4284d9ecd46343000c1e2d6ea06f2d95f483ffea1902fa3935bea0e9adc40e85dfd1b59a597f2c498068af0ef4c15b51d535e4ed1de28b1b1250963dc00a70e199b48d8d7921bf6cbaf268e801eb241bf659dd38643f39de8b9e0710c22eb45780036ed3a86fd4b9c745d26e2d3a5b7e87ef6ac54d8d4f9d7d01412d940299fa1979716de0ebd7b26bb6d8ba4217dc4a660ee24a683440a12b00ac310b1acc6481d42656ad0b08eebe4883db71a6c64603e07f402829c2677663ec68fe1e7620b6fed23b7cf2da0f09773b85db63221fbc6550a7182d7b9d8b72ef1ad1"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 256, 0) #2
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"5aebe22736577e69c5027cbd1dcc95146f8dccadf961020cae23562d70e9f0155bfced0ce2053114972614a45932eed8a6b4f4e746d8d9e8b25cc9d9fa67ee0b15cc5b3e3a2e4371a448c9f6bcffacb8a0a8f2c05e8a3a0abfd5d803a77a80fba75ff12cc0649af9bcb94fa5ae2edd2a":"3422191ee68de00c779434aba239e3cd7ad535c13d118bb226e1e013ea6e9511":"":"":"6bbaefdc1aa307ad401b6040da2036d6beb5c53bab45d72f4c679bc88c911fd2754a09f2f4b4ff37e7fe3cbd9cd788ea89436bf78817fcb3a6472198b675c837624de8525dedb7a3b7901faf8dd09db1216f55205e3719d31103379abac3a0806fcad0474b9bddd81e3fec33488893ead828e08291b0fbb37a12b74347d35131f1bd51aa4e4873096b1a35ee3db7b027fc5654e5a0352c22ee35d70f65b39a5b8f4a206970143d55f0e538fe28114fe3963cff7331e59dd25c1676bcea40c7074073a95b9cb044e114456079594d5c570da4e948bc35be44a524d79bf4c8155720418b8e7ad60990bebf67ec5fc083dff0fadd3e94ba110de23e8ba699c81548"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 256, 0) #3
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"f5340f1fea08877edb309b9b43228f11dfca26f340fa433f0b18eb9e6e07ccbe96f7a1d745a9b2910e21bc9522a989dbb2db642c5e4b2d59ffeed6c9e667b378588849338b385625f03a226389081858e86a222876f18a0d7ff69d0fede620a83caf254eb9376dac8ef99837dc491dd4":"98f5b7af38c1fbac43fa9cb358bec11923d103720a73591de2c6ed245e86e028":"":"":"5293ce6891b5641a33199c0a52c2b5ac46b261ed311d15a6eaa8df6478b217aeec221d488af74a347ac9a14d51e07a239c2a52d2db6d75dcd901452fa3b3403a15c449c2f1f9770501fe10884ddc3ef6db2d89ead176dd9d240446b5eaef3737666750f56dcc4370720419136b0e6268efa538c7468f6b21699d68fbca51a3c941df46fe9564d395c54d829a681864837fb2b6eeecc994478210317d5908886f6056293d53501a726cf4e786c6294381fc4af6e1109186759ec90999d8a21ab09053938fb545692ac03c776803868134c3e4f7ed87c9284cf16a7651458d7e68b625272687944e2e6c7ccb4fe8e003abbae93f98f694a8385a295c336b5a404f"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 256, 0) #4
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"82738d1234a9393fab94ab99b841371f7046c6852bcdfce1b2d56825f5c58786e599005a8a79a30d89a4251d3a797cab8b3f30950b9a15d686f1259a11a516d399551928cd3cb5734c7839847bd584c364b95b8feb390567cb2ec23746543ace1371a089ed97f9968e83e75636203574":"3fa319b90a1038b544916123534aa5cb10f4da16cb12c3e00bc1306423742bad":"":"":"9bba6c3cef2838d115f1030925a01db7881df7e7b5d461a5f8

dfa2a40795322df746a25ebbeff272d064aca9ae284b50b6f93fa566ea519e712c82f5ceb481f2ff873e73043352c764723
8fe339336cd7aa3765882429a09293267613e29bcce17535efd1cbdbe5e40bb21bdde402e6ba7d554b30635d05f581dd
1bfef0565c3f5dedc8210b5a01a10b58130442e3f8eb11b9a40e599ec8d5e1089ef1f5e6587b4120d1fc39576282c80c8
25e6e9507a0ceb3d0460832ffa079fb8492a3518f27f09c0bbf06f6ec00d80e145b5e848b688418419cec8ae52cda766da
84a856f94a4bfbec26a97e2810fb1dec3b48f285fa4b0e2794fcd28455bb178b3d55340e"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 256, 0) #5
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"e554287587131cc3297b05c8adab4610cc3d1634eab65119d8c546d13e9
961594f9e6cc618ea0d782547d54aae466fa243c2265aae6d575f8fe22edcf71b3e77fd9f9ebb11c9e2e81c70abfb19323
9adb73e4fd14c93bd84bf79c328a86a433427b305a6425dd5711d83006dd2db95d6":"2a5741cd93041be381636c081f
44a9410647961ce5265211ba69e09beb6e5cd3":"":"":"ab0f85e64e334bbc741b064a31aa9cda9049dee0d6ea68d1483
a60e0f48999527042b7994d7a7131423bbd5a6cabb35b9c78628034fe31e5cc2b8ea2b94c91a488fd34fd344bdc862db
00e234677fd0fb5155ac892c304361e0f5453cd2598115cff6a3341200ad7469fc5ea1eddbd85511cf20b842c997dbdf9
5e4841aaf0d365080a24faa003fba9226bbbf609086a6a378e5a5c2682ffd93234dafa69c2594cb53e77d04ba80367ee5d
c92cc606fdf102d265d52a83511e2cc1d166f3b84586b2fb01f8c7ed39a344a40ff884e6a3f97f9474977b74318d88a6c7
0b8cb7d2489e655189fc97cf1384cf3927f608a1f451c77060f4309ff913f89d21398917"

HMAC_DRBG NIST CAVS 14.3 PR True (SHA-512, 256, 0) #6
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"ee071e3f09552a53b8bd98d9e4b4b460577bae8629ca6e8461111a1ec08d
5188654042148dfedabc409caeb5a03b26e422113d79729e75ccbe2466ae8197cf8ed14dd2a9382596da6daee3314b12
ba42cd9ed90aafb911598d1863c9a72625d0ba9d711d1fd3dc462516a6b6286644dc":"fdbdc11a4f71667bd1561e87ee
34d925b13d1e79967fcecee8b2656f04d6d379":"":"":"acf342f6537c1c3a8f050359730c185e2beaaba5686d2ffc0101e
3eb2b153cc80ed5e8404bc849e330e980c0c2ee5df6e630b0d2e28ea50f9f8c06acc0c880304e321ed7205e673e4bb44c
cf12ee27bc6f168b636d4297d53462db1c4816ac5ad684e532f35a21ccc6226dc6481d649158e75a6eb012eb95ff4b460
b41f8ee1335fcc43f0cb9b5ee76a471283ffe0880e5cfa2ac200b18149712aa10b76fe3850dec22ef4639beeed69f01a4c2
5ce6110a2eb0a69c479c97a6ff2be4adf3c725511f932f86419ffffd0306bcba149390e1d30679c4d70d15637665419d17
e508c0509bc4a1e73448c29df6944c00ce8e32ca8964418739734e8ba0aa4de20585"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 256, 0) #7
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"e0bc8c0b53acd8cf5e4c87ad24455bc34d456367bd2e71674d5ac59d0901
a07abb52c4f264b0607bb8f1ac0efa4f974947bad42b482868d84208f064fa27f465865b910d8e536f011097bc0cfea07a
934ae5023ac7098985c4e1e2d173bc835f7f6fca3200e38482a36c871386ff9b0d":"bc98fdca1133a21a2b4435105b1f9
6be16333f5ecc6618c54d28aab599b79549":"":"":"ec616993a60d7971858ab2ecbf86f613ad0d9edfaed886455651 59d
ed90cbdcaeca3dec081f55857df77a3724f34e797729493e995594de81bd1d14f55fc76ff1c99e86f4bab5b01cc849180b
c0721bcd7a1c694a523baaed436949882daefdb9f555ba163bc01780831c06fdaff5bcd58c61c08b39d051da943a1a3f8
31808ae982e3bddf40cdd47d580d3be6603c7818614eb0cbf303c6e6f7b52183e03e42b57153e9e0644c5ccd1018e242
fb384d8327475b6c51c32b3dca5f3206953963174775730105 1a0eb4c2e4bfe6576ace08efc5b4ad888a4b8137797cc7
4625b847a5b6fe515ce186fbfe7a68ee1dd5796e7aa94e78a85c5bd46953d8c4fc0ea7"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 256, 0) #8
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"9c61a730a0ab38830f36a44181988afa24fa5de5f298db058fb4a3443d3b7

1412ebe35851a12f942b7fc379ca1e14c6319cb485e125dde2482c5632976a2a9c11221a9fb6e65bad990a5b77b55b2b
8623a5509cd919819e7f8adb23a99b27c2d05fb6a3fb3936d5fbfd44cf2b24a7a87":"a60b8962b18d686ea141e0f4f015
72a25b69acf19740bde9588ea63a11e904ba":"":"":"bcad32168d8bec01482534ef7dcf27ea111d6b2a11311572e09bc2
cdb376f30157ed19b90baf8e4e3c61e6f8dcc05839fb1b3f1a723c3ba9dd1c7cd49463278a6b2190dde8ee03242d1be9a
40b570dd4c30437f0b15798874ac940dda5bed2c93323f1e79d54ae9bc86d82601987f048976a557c6173f9d3eb16649
bf0044947206f3958af2cda743fc40416e645b9596b1ef4e7060c690d75efb4acad24976869627c20993d89359d39cb3a
97799f9c9d37dd79d212c690cb148d2b3006cab6d43e798aae2a35e8094a21d632bb05a89ab1b6853f27b7e064041f14
0870a6bd9513bae4c18e791e2d8f1b3c7bcfbf82d28c9d6cd8ae224034c306e51d362e9e"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 256, 0) #9
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"e3d186a9a4d9530906c58f9d1f3b415d1b60e2f12ca34a428d16fde09c70
0dc5ea9d104a92831936136691232ef64c887b71383be1523478c67387441c67fd7761e9f75fa0636e5a3caa845219f35
82bddbd0017b9b95984cea6a3ddbeb0820f4f55ff15e22c00e8db7dd8fbea8f6526":"c33655a0e2973ba13785fe4edfb7
5749d84d818752f7658014448b7719982726":"":"":"e002203e9dcb191c5c0c3ca2e143e689ca9925337ae04c29547a5
6d4144b2657f826742c2af60a2ef56b4f76e68ecd423ca04eb79e92473c2b2096072918a2390b5e1ef596ed6a4302c181
b03257f9defacd58796e10b5601ba9a1be767440ac0aadd4f647bbd81a084bbd8bed5a0091892bafba61259a46cea95f7
be6ac76492a52957eb62e0c96f5dc74dc3d949e74310be664cc21b9c76d39101b76b7130f2cdf444e07bdfca000819dfe
fc2eedf897b1de0ab92e3d04f6dbe9438c71115e5d14fb663d712027be4c1348cc3c5c30bf8dc0f7f5a2456159a542e58a
ed5d10affdfed5b6eae77f3af607354ddfc4f1d7afed90463486f60dd9fbf10b32f6bb"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 256, 0) #10
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"38eccee965505ba5136a8ab868ed1e741d343ad713075233bfebe196fcef6
f4057a21d8b2d6c68abdf52633d54d9609e87542efa8f4b46f40a4e60a2dbcf3338138d46c1e14d6f752954a8fb992fb02
60ca8890300556ca7092a7661b65fbbbf0c56e2d49875528aed1ebb0133f13c55":"7bf2914afa8ff9c3b384cb495d0a08
bf7d8f0b7198df96db7371dfe987b2b73e":"":"":"830a9f61e8af4f322a46f3e75d475f9f6d076713ab98b2b9d1196e8fe
a098bb7a840ca4d7f32a850cbd7417297211fc37b47b068aba349d26a47b2d6d41e5883f656c287804fbc854521989c5
de99b61c58d5144440ccffea4a0d9c455a40d4718cc1e9dbdc9c77c4848f466257f99ab6073dee83cf862511b68c2bba8
bc907b88822fb1ba310b3901d7aee1eb3eeeb0ae5e8da38276886cd8a218d26a8d899afdc233944c97baf7b27444e27f9
f3600b6d908fb179e504c5091e2febb7478b34bcf881c55fd9fc74e9eae1203e097ca67fcd62f03a1579d898d890c57445
d9f6ee1b65b2e1542f490501384a8b98cc598dc8eacfe2260db6d65c54ef915f2db"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 256, 0) #11
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"19222f7886766642da4a80b97b9ab8b157b58ed63dcea2512f088644791
475a5c6a33a2cce394d45da2f84b02a0abcaaeca4698d50d5bda435778b808397315654878e866ba0136f9c4e206f774
9b60ded4198d69d1d077564a894375291991eb125d394547d226c2da17e8cd98853e1":"af34763c141bc212271d52a2
60c6d6d40e9f40a8a4cc3fb7ce6359bc71941f89":"":"":"5914df97ca36accfe40009f033bc6cd2195d0b1d354960d152
157f2b868db4cbb736cdd0f077f230442ba0101789c5cc2ac727b0704a10b41c87d79c8aef748567a2eb6e61a7c499a6a
1cd6a9d958cac18585b2e697dae4ff92bf913480968f3b2b8ca2e0cd85f1d9303e3a1a3830a30d6ef0a1e02c682958fd18
6e1be8ffb2a4a69d34bcbe617c3ecca0a77d460e3782cf10143df34adeaa7cf74d1d86fb1ed35da217f00cdf27f1637d2a1
88c3ce7ce6cfafda3adef4463a0e7e668eb1268ada8465ce909f368a0b12a439eb4d43a87cbf98f83a4f8c422ac90851ed0
81d74f212c854522437b2655959c081fdc8ca2945271821182691f6ee5fa0c13dcca8"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 256, 0) #12
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"f314eba7451a0b721622be298659a3d253ea5925f5912196c62ed149daa1
1e26cd94e8e647da38bcbbeeef1da21ad92e0b9a5f1ad72826bf55097621314f9859f8f8d4d62cc9a00b3e9d95e996509
d77413449aac8f9d8b311577a083f80364ad1d489262058aa11ce9fd3dcc6b1e4cc":"f8b1e97ec680f637a4792a0d50fff
9a0edb028619a9dac05b8ba6d57e55a1a4a":"":"":"93db5a7ed48a819e9a237ad4eaa33946880ae85266418a264ec17b
41a8c97c16c446f91c6d901871e70b6d9c10aaa07077c1d40242cb7c5cb89a137094aa81628278b9e453d7f0f0347241
10acf8a08fa244da256bf3e41960013e70974dc8c228218cd88ac4d7448bd13a4343866b656b16aaf42ff678dfb960523
cb95776bfadde24e16ab0070305e084cd970093fcd08431b815f85fdc4f6a43fcad105965b6fb1661c7709a166ae6f3d1f
b463689f752811fe7d6665689a06c60aae8a051abfbada40fc602fea2ced51aa910c09b78d97a4e85242c3d206cf31ccfe
e11c5dc141ebb5278b55de7e7aa9a08048d5cad072da32c449bd0dad2f7d6188a5b9a"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 256, 0) #13
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"841cd7bfc5d87a0fa624f474af6d8ae9f2b5a1426cf1b752ddf11f792169f2
f2c0b60427bf62df1b373302d91fa8dd891fd7542bf6425a7308f64e96b0c3e372d4addc747898731517a418210813f6f
14d56651b2599bb2899b109b9c21367126ed5bf099f455ab5b67f47a1a3abc3f6":"c35726206d18f9fd3b8423fa9ee2fc
5a896a013a95d052ff495b9cc6759d58f7":"":"":"b3eb113c19f33eeee3dd53fe58acbef68b652121f39e9b88472e9162f
3429c8d98790405afe1368619366c88a487518e1ba7896eee2b4625a987d138569892b8f977798d6931b5d2fda6b8cdf
314063e45a22c957a1b96a249c431bfcc2864fc00157fe6c2ced99a1cea466944f675e52cb8fa0027ce78f4e3ed72d19f1
25045aa824b57526ed20d527d371475f389c66a15e35c2ad1bb8a79842217a422e4b73a3ab5bc8cdac32eb4b1204520
2b1ff1323a6816c29ad0d65c9dfc8e9bb841ae0c813c0bced097877bf220961c0447162262a96b95dd93ee707393fa5eb
a4aba292982c216b05a8c2cf165b54e1bb50a9ec20151b229df3d32f54ea62648b340"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 256, 0) #14
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"dd62ed0d54d930fed1cd7582e376ab47da3138f77daadeda32fab95bf881f
e90d9ab4dc5b1cf0641ad966ba1761aaedebad9ebc3f3b24688e16251c409267bec9b02cca6b8ea7969a5991ef647fdbe
28d3126c505bc0d9f8241fdc49e8674ffd6bbdcc5f99c6e20d4271b4215e224156":"366c8ff666c2b42d735dcca5c0b12
e352afa483d48d57c908b5263ad3d2affbe":"":"":"a774564295c318615e4d66e0d857dd6290ae074cb38b6322d8867f
2c7bfb7b3bfc50c715c090794d794aae12b6aa1a91ce503b549d79435fd1f407fdbe286e4d607c624b44b5f0b91e65aa5
9a880c695a0fc2c9d53dfe0662944ad458ee6c364e56e6537ccb62deabf1321e8443cdb58e8833b708807e53ad86eca98
e7cedb9bcabcd998f975b9b8722125da2d7f8e611b48e7df63ccd44439c615fc3bf237561345d85378a34c46b65bf5cad
a2e1c591f5a5ae4cae06bd2314bb5e5ba067eb65205aa2e4f625be97321a91d964c4be9896ecaf20aa78338627ea90578
cc900d2abff4b50aca44b24088747e7e27ba9605bbd6f30c99d6697be460da653a1f37"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 256, 256) #0
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"3aca6b55561521007c9ece085e9a6635e346fa804335d6ad42ebd6814c01
7fa8aa7fd3c3dd5d03d9b8efc7f70574581f4cc19fae5a456f8a53a656d23a0b665d6ddf7f43020a5febbb552714e44756
5d637386b3ab33f78fd9751c7b7e67e1e15f6e50ddc548a1eb5813f6d0d48381bf":"4bc9a485ec840d377ae4504aa1df4
1e444c4231687f3d7851c26c275bc687463":"b39c43539fdc24343085cbb65b8d36c54732476d781104c355c391a951
313a30":"b6850edd4622675ef5a507eab911e249d63fcf62f330cc8a16bb2ccc5858de5d":"546664042bef33064da28a
5718f2c2e5f72d7725e3fbe87ad2ee90fbfe6c114ed36440fbbccf29698b4360bc4ad74650de13825838106adc53002bc

389ee900691649b972f3187b84d05cecc8fd034497dd99c6c997d1914b4ef838d84abf23fae7f3ac9efdcdc04c003ac642c5126b00f9f24bf1431a4f19ef0b5f3d230aab3fdf091ba31b7ddcacdf2566f2cfab30f55b3123e733829b697b7c8b248420ab98ba6f11b017175256368e8d8361102c9e6d57386becbeabda092dd57aec65bc20ebee78eea7294571e168c454066d256b81bb8b7bb469207a18ebedbb4348fbe97a4d86d2bd095c41f6de59aa0800e131e98181886a2633cdcc550914d83b327"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 256, 256) #1
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"2531c41a234821eec46f8aa7dae8e3ae12d167d289bfbfdca928643b343eb951015c066e2d278ea39d2a459e6434e234e55fa1145583ede74e632ee8bef2a2ff76ca3b8c9c977a5813c4041f3f9328be6c67f1689d878e8ad61bfe6a39f5b034b75c40c9b305c1eeb92a3f4169ae1720":"d1952b7d0c4c94185adc025e67a29fda50f577770115c0931bfb03e8101d1d3e":"0be3f61ece380d63c68ff0d4bde36f58233358ce62c7bc588728cf1babbd4342":"01e76a0c9addb4dc2001bec231b72e2098a6e9e8d39ada13ff0c493aec8ba65a":"12336758fbec11ee264b06969bb37ff1d37034b66f8b823690758da074d4e09d84ffb493d0610b5c32f68b1a144ca654ab4f0e89c89c6ee6b872b6be4ed06a77b9809e68329addf4ebccb986dd48cf33469362af9d8f7b24aa1cc65bdb814c2e04b79860f2d53b3895b5f92502befe31729e40ceaeeecef456dbd723f485082ad475e46f6023dab6bab0eef61394823122c262baf562d55c687c3c3408c837e6383e11535e950e604df59cc0af1177283fedb5fe30966460dcf6b1625b39b590d455b9182097cfc143290556d68158fe20211effab9303115ebc5b699dc1613c195956dc61348bbb525e571c5407326a6e1628515c9275a6a5e35650c953d68f"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 256, 256) #2
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"4d65ff2fd260eb6290b02b1fd71cffec840cc01807e984f07da64e6ad80ad37fb5810ed012d2ceec3a0418003a03343502219bd422c08e0321bbb86d923bbd04082f939ded421657f929b37e21604a2668b57d5606ac36456da916df82a8753d224b4f7c829d285254e9e851937b54af":"d75616aa0190a56af573e43605157c0e0d5275bca959f2c75d0e777943b200e2":"954fdc652d0bd8eea37342f5547241afb67f8d4c587bc2402c435a260144acd1":"ed07fea3a07e8846b4c3aae8cec0bf6df7c8ba7817e3e9699943e2d2e778c4ac":"20c1c41c0809e694b5ddcb8089946d74571144473dcd68af68cea5881859ac803c0192304966a3a6f4c24de0451451128663bafc20c9842bcf72f3d6294dc59b850dde77ec9b7b37d8e5a99ef1719ac29bd54027278db159476849d22d2b46ddc008cf76878eac8c709066aab5f1043ea588815aa48456d89d2657d2905422857f6b741218d22fb7a2a67e7efe5c2c56c9224170a75db10b9d7b93509a6b1c5e9b6d5faf354f79394151eaea71c83c8fa53446eedf70582c4976a4c16311f92cf7d1758c1d1f48e6d58b588b3cec5f2a7f8552dcd7a72cfa8f109c3f734a708304bdcdd6b25acc00899717a05fe98433f104b6fd268379051af36b111ba179f4"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 256, 256) #3
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"313680a6ef5cc85924575195608f3b9cd852004343ab708e89d61c24696246166b0dbcdf61c59b0041fd2c55a829c99cf8468552aabddd993687c2b4a6017024c41100510ee10034ba4f66563db4d3388a7f6d475e080faa23ed43c674254bf9ed25f73109630647fa3c85575727d2e1":"cda08cd76f3bac2c30bda2069a1a7a461f2462ad2b2ab6a727da6836896a4d2f":"431c4fdeddd3da1de6fcf19a25d74af811f72fc2367a7f33cfcdf17cf38fcb6e":"4750344c23e4686b2bfe2dbd9301705d06969fedbc77841bf6591540aebfebd7":"40deadcd87a8e07ea73bb1f29157c7ae8a35e02ee60f9f62ebe3ec4bb325c81c2a17bcf6b863cad6ae29356c0e7f3d82052802fd7a14dc73954c78efd49b2d32f072b137af16a05bc97034b2102c25d6ae68df7141b101f468d790780330157633 26dc3ce8bb2e960e7fed09905044ba2164deceafefd545e67a5715fe7e5a1fe51cc356096344245d431dc19eff99b402981b8531a8702f2ff1bf268716793367db8d0f6f454db57b6ae9164596850811fa2bf01dfdf91799b1b54c9773ddaa23164484fddc2cc781c1ff31393ea

203420ab2cdfefe514d3089df1b20eba32c003576da5a9712c5c0ad744fa03df197f2ca8463df44d16135f05e1eab014073"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 256, 256) #4
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"95b698a454070603efe15cb4c359ae946da756d124939f916d67d77aaa0608d8e577b5f5567ba3c075128b528a6ecbcc2ff6d8d15ddd68039173c4b70df3651f4cb5ac62957781ac91563324a56b47409b02699662f68022be2d93eac367a21026ae95ff0cba67a630e4bd8e53469215":"de401ad1d2c339934a47822421eba0fb79c89863d1df0ef5d47e6be5bb3a8c48":"a002954ae5f7676a3230533dbdf59252ef051acc76574bd519ad56882bbf46e6":"5e3de2b53936a7890db7248802bb95e9093d9d7a15a9378d8f4ba42c52e679dd":"772a05c279c7fd85750793ee81bfc32719573ec519f5b64b0386e6414b73b153163fdd1dab6d22c637397a30adf86594de90c32f6482d50539eae8775799b89e4c6471493df4f90ce0b694fe1a81fb5b93bfd2719ee69cc576e632cc886824deb7622d487af450e95bd55a609ac30e95adde47b83ac654474c18f615dbfda68267cec8bcf70d094df6301e858d3076db2a85b2b4b3d94de82a6e0720d535d36d6e952811cc371b1e828b86fe00870aa5c55e575a6903303f9e2dbca40e5b66326192f1728bb89fa7d77e6d32cbf5f18b3306206c39697b71c404e38d496c52639f98eef9203baff52837a872f7688b53318c870d3b8cb024c865c81c3ad8b71e"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 256, 256) #5
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"d7d3e83dd979bcfb524074f12a90f78873e983c2aa90e0241f00d2c691a4702bb452dbcc69a7793cc2081b984033295c4435495713c20295aa97bf42babb66edb4856370b9701020a8a79df7381650fd7a3aa5ace4bf54b3331a8d4092c19fde08cd51a06146cdfab9e3a32e5cd02b35":"5612ed7d790419dceab4befdce6e4e687d335a3aa972d8809db6291e3001f825":"915028d0610160a2516e926f06ed34b18ad1064b6efd56566494a92a3fa0eea5":"86cf5bdf061711d2361ab6d79c731c2fcf9aa47ae5bb5f6294486a14081b1862":"cf1b0dbfc3f6f3ab526299b7f7d8ce1a945bdeb0c0f6305cdd6876d40d5649ace9e78fbe2e1df6511145635f5acae90b6b9a38393db4bdabcb2fc5e93d252a2098fc082917b1485d387ac5e2efdb5fce0e82bf200ce0d1f6c7b5d22fba062574d9234fc9185f096848d10141ad39571035b3769a521165f7b63a0050a22485d8a47870028d3f3b6437938c3cb51781db9fda64019c049dbb7335dcf7c9c71f1ccf27cff4d379a274fea0d026f5de1dc8866f1dcf883e2e0fdb6316059d5172a6c1faa3203969969defcd8f367ce859aebf998349ba979afa5e63d94588ff02e3a428e93b98464997829cdd4b605a44393057fa27a2fb780b7daff4b64ad73b91"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 256, 256) #6
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"c1e64b99394e1241b31ffb7b482cfaaacf5f2fbc251f954e7e3dc0866aa81856a16ce83d9ce70b71479ae9ccd6c59ea4e99986d1e09ab16eb1f48b99cb9bc9d63701f6a9a1af0b1d8057339d5d7ffeacc8e5729134ef2148663227e348dc31b9d56626c0d43478d5d53bfe998fb85b1f":"42be743f8a9c0187d2d54b596caf64dfa630d60bd8c6de0b126d6a151d823cdc":"e925684793bf51a8a4a46c2ac5b91ed40843efd0878336f983f1001722231f1d":"df019e78efc5d3a85fbd9056ad05f97de81be05c069b32e68792ba8f5a775fb3":"cc3df6f1cbb0e1bd937e64b2d8be12c07cb256369040d834037226b96e4b8e7232c2abfcbbdc0bc2c432414845c5ebbc35fa4e903d5df19aef62dc702b20d0346daf20caebd8819df9210a721be34d9df72603a4370c0c6a653979d19282505d64ae09e0922149759ca0f5324f665eb83ceaf6dd46771c520b96885a8503b6be333ef6aa8d83d370edf100edb13b86724234442a15cc23f89359f629a2a15b645c2510099c0263d25e310567d822bf03aebbd4bac392b999414bd013fdb00b4fba8e30afb17f50145d11302d71dddad30ce6678fbede83e567a97f4deb3b1759e191319697efd9486f2b502a94e01c00a9b5b76230036665fc5d87f8c9e2fb4e"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 256, 256) #7
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"071b46d52085a658309f2c35bdab443e1509aca159c1fb9c222951affaf1a243d0bdcfbcaa247fcb8da53fed8e5f8b3eed2fd022c96bdd6e86bff89beaa99f2bc34963d3ef118df9a5525a910c9540aeac5166f65f5d05c6277260081aa9b71ac58cbb5f1ba5000d4d8078c5a30d282c":"7ca33e3345bb333a5b1f412a6d57f8ebad65b427ccbbd7fe3ac837691da39219":"60efb3c75aeb2f4fb208659f20e79eb41d8d9b422066c235a14b9420bdf6f172":"4e2675c8009b5bde9882ce940d42daefe402fb11379e07db9a4c0c763e97f319":"80b56a4bbea08b2bb09fda9cb04b1ee7bda0164c2f12271d8857ee3af102ab25c56836354052e3d85bb02cf13607d746a62b24eafc989b35d4ba25449823bc1e7b14937523f96713c9098ef2ac3f9765070076f28d76c7e3c2a0fe7b6afd0ac2167ae070a7ff19c5bbce52948abbe94f0d55a5d1beb31a665e97f56f3b92314cad9ba764cc2e3d0c00064ca1b4f3efda14e7e0aca431b427dfef2443d9e3b8a6567c26eb0ddb166f9dd247371407676c6a46fcaa0f9f67f49276676369b725da29aa9ebb7c3e186de460452cc81c02266bb6e79a119c54f4bed8bc3de709bf6a62593273f4680136e95d6d121727d9fad55c4a110a08be1e0a06cdef98aa04eb"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 256, 256) #8
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"06c7a8a74b6fe9e14fa2475ef8b8a1ff9610bfc1b4b93cf53a8c844d7dbac08ff743ea1bfc6c10d7707b5172a29af054491b573dc2cde1a3e74262f4fd2e9ec819ecae830db4f0c7021028737ffc5bc025a216f658065e27314c30c04925051c0d7caf6ef440cae263f49148c0398007":"1a33793d255386d47952bfc1f63ec15caff3603d5c28b2acdd799673affab589":"7eade98e717aaa32f74b033163ad76489a7d682783d2db67b9696ecc7b9be57a":"58369a241166bcc87e713b28b4ae216a8e61f8cba83969d42b91e55283286af6":"7bc84544b68eadac9cf1ca907d9166e094844b396e5d54672ec88dac573418125d50befe1097e2f3438aaaf3f13182ccf4593bddd52d6a41a5e58f267c6f0817d8d1ce3327a611f9fc591ae64c7c18d61958a598e0ec4383e25b46dfd34db10f609cf53ed76c86116018fc8e9027aa2f0b0fb3f22d6b86b11311daa5e78d1f4105ae4ac67f63707400b0f054b6f3d71f26ca5d463192952fb39ae00326db9cb1dc028525c31aa9beb7c3d299070cc3ed8279b8ca32940b21273afe8016d8069a577acdba6bf6d2fe327b2f6dc9c5c7875da6c3f584516db0365d16670db6d90cc1e5bb5309ce9fc8234326ddd68706e1d76830202cdba770bd40046b751f3c15"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 256, 256) #9
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"d5552efbb7f33481a574589c4bb56dbe43000ffe9ea67fd0c8d5638092c8469944a150b0dc1315ab0484976b128ccc961734d226d66c77dab3c22558ff2225e32191aa2dcec8e47a56f757f71c081acaf5df357c07952cf6de2e3564813ded982f72069ed1bcff6b48ba4b4625ba247b":"345b4acb2b0cac82139fd516ec3d39292438a916d2d2c8e97ef265a1192a65a9":"732451ce7bf5acc84a05de3474b622d07bd3d01eb6e3724538e454c4d669a994":"7c7ef660cebee96b425485296a8e88c37c66e385eb1cf7389a95c46fa68a34f6":"d82473db3bd554cdcb2aadbaaa9c919087d9b7bc8d883f99bc95a19fcf96f25698fca8a134ce441414852166998a6ee2f6a18f9f667907f8f8bcd0d2ade7dfcc03cbd6ecbcf3dec46558154dab59717f386bb33c9df9456b258feea593ae1d9bfe70799fce4b25cd6ffd0815e849cf93b496d6ef36cce4e14fc3de1506dbf34f7111b48027ce2aded4140bea8311d5de9df5290e80fb65462fc5433e00c344a3657f47f6a7b992c6ae362afd462280e7830d317192bd8dd26dfefe779dfd69ebfca34038b078c01644857c60c1f6db9da9877cbd2721d0b26a67c4eee1bc43f6d632110759e1e31e7c3d6105e3da30d297b69eb04e880d1f2bff2a54ea798178"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 256, 256) #10
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"bee5dd72828806929757afa02a92c5c54d86c5015047379b717c6608a71

239b15255de5a2bd27e9c6ef23046c8a8217bd89744552137b24d93e5ed41250ecbcf6ec77734fed7a40680e801ea277
e8c6eae57b4328acb1e1dfa04d0b5f799ce1e2f111c3fe8c9f954fdad6aceac7d27cd":"4c3c54284845fb2a494d1e452b2
ba1eb0d3456cfa9560ca7c60878e8458eb7f3":"a8a333527a2158a087879a6f950d2af8d093c4f67945a140549a5e93e4
05b886":"bfa0025ac9774ac767a4d3810c27a3c8e3e48780cd0597a5a401f6c9b0067e7e":"ef4c169fe5fdb37142c7173
4b5b5c855a3b7693a0d78f48d76199aafa3d399b057ea78b2f1187bbd3215bca52e3bcdfbb74d1d0c1fbf91e7a81f7c3f6
d8ff5276ca906704d2d3556ec8ec1d6d7ba9e7dd73738a7e90b1398d800617f3a5487179439e25d0a9d4ec4e38699b37
03020a99c533a6282000544296e63b6ffe12dcaf3864a8502a68482f90fa7fe9aba6ca9e9a74c6e3f89541d18f2a909737
280ac8e772fcce6a117411f36c9e82f2d77fc7a03e2f13f97da5bfd6bf69f1d46a64c519046e6d0d379964723bab2b89be
9ec91a3e5a33c53a73304c1e89620188aa2e0b8e4112c5699e6a99d66b395cfbd2502e567a0a9e35ede140681b2ffd95f
e4"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512,
256, 256) #11
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"754e542dbb453f10f41e1361164f5e1ffda67a024ba26701cc86066caf2f9
477a074690faa069cfec6fa38d8b2506aca34fd27d66708876f28d8ac08d28eeefcb728fb6226559d5a0646a8e183807a8
e08469cc5535712a4426ddc5a340b6c71607ee1e2df489528a266b141d7c977ca":"3a9193fbb67a0fdd732a788d3ae57
83de84968794b8c4c0b5ad4de067a5d1fe5":"034db3c40c2c181cb4d635aaf08f05e724f418ecf7b3d2ba6863e9ede616
857f":"50058bcdd53c9d257dab7846fedca4ef99ed069604002cf58ab27014ca7100c0":"1d30904d8cd4e37357b1b9b4
ad060fac12d1cf1d05e2b5b2fcc48bff12643b60f5e40a3f3e542e46804ddb904581cbd576f0dbb4b83b49af83c48b6c68
051d7c7f4bbf09d3a4f999db4776089cbed57dd2a75be826ee34e13dd802d7dfa4442a0a0fe154ec9efe6684d6a400d04
fa404123ba54d6b89b7dfeca4d4547e3197218dc36be5c0137c94b889c1aa22b7567887551eab168d365d11a5fbd0eb1
5116e929468e8eb445608d91388a9b3b05c95b9733bb3ff08d96c0899b50b47c570d75323c4d24062820b0a9afc7bb2
771fe163ddceb411470f33554822e30dfceeefd0798ac9e4a48b8d30c8f725a4df6568d15a750131998e252dbf9199135f
817f"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 256, 256) #12
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"42824bd8944f49479f07cf6af8f02aeebda3ac074ab72a9eca8850c99b909
d081f2382d4ecc9e923bf1a588f8db10bdce61c6f452c8e15c0f003d2231ce5cb69292ae1a37c602aa889f0d56df049717
bd99005ff353c08eb29ebb8cee3aafeb52b3867a61a76335d86c2d7808ac94bba":"2b573345c4fbdb8382bbdac1d3e2c
38fbafbcb599c67412296fb6912e1a640ac":"a5f43abb4634bedf1b199dcf6394bd3504ffa0cdc151b4e53cd0772d86a4
3f60":"a2f1ac52ec46d93b3b944055b7205da8fee95c9a3241418cfbdfb0e9ece9143a":"c751240283ec2480f6c7720c3
1e1f9f70c23907b38602ff74f707a14ac10989e29d1ec2e81d4cf85a9bd3440f445fdb9ef7955bdd2beecb5f3c69475b71
abfb4ebd5134144b24b011e2fa6026d84f8fb511c7a44f2ad7cd212acf089dea4bf2db5be9a24cded5be8ad0b8ed17bbf0
c5668fd644daa863616f68278b5f6dd95ab238451966bb5ae6679d1e99bad610befd419ac6bdab3440b7001139af8a2fc
a35c74ae65d05f490a480caafa1e3487b78450a5ba59fc0a59220395e14685d02f6b4180c72977f095e33c5cb5048b63b
cca2767061c97c616f494c775c5d37a67c5ce996e94bb8ffde4a8dd3de97b74493c9b2d985a2492e1f97fba947d2940c5
"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 256, 256) #13
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"9d899a56a0660f18b98c921b0d409550fc225ffcfb975e9ec6b2315bc9a1e
b3f68fc77abc3452380e30ac761a20a91565f5ce875a82ee08a46a1fc5d4aaa8918fb23970428c863dd1b24606b011847
6b150f7a47f3962dfdd8ddec93fc8f82df7cda58cb3bb5623610eec69bdd0722a0":"67bf61b3eca94013fc165b110eafcb

9126917a0ce7e2d9bdf7ef1b38bab6ca4b":"db144f531cee5efadc505f4d37a6e5413f638d46d419fbac76f81ecb63ea28
09":"d737b2ba62c1ec1c766f30a5dea7363b5c570c1e7a33fb65c3fb89eab41f748e":"de518ac3034859a43cf67017225
55be929a5ab2658de326696068b970ff2f77c75083fee45a6660b82fd1e960b472a50d96535559f60b3e3131a2e051af1
18063c1cc8b1356014538e6ed0e2da05c90baa041085f8f1575fc3103293a0303751077438a081fa3bc5c64aeeea5c4b3
4fb6957e91db47bc3f73710087db9843efa1a62e9f615843f69f3f450d6c58b33b1a4d55509df2f34b8a14407cd1a87dc
9581dbe180e2d839417a4f6ca6a731aae3f08b515df8200890baae9b79db798c8e530b6a03ad13c3c08baa4cff0b055f3
5dbbc6cd08fbcac7c0fb78f8754921e000e622ce3042e740c64bc935aca85d7132723de8453c543d5cd5a40748e286b8f
"

HMAC_DRBG
NIST CAVS 14.3 PR True (SHA-512, 256, 256) #14
depends_on:MBEDTLS_SHA512_C
hmac_drbg_pr:MBEDTLS_MD_SHA512:"ae767959378e9f031c8f68d778cfc0dce1f9b4cc176c5f9f9f4c9c3aed9435
f482585a0711812c3c79bda619b942c6eb8f5abbe8540aaeeedeaaeb52c156d07d8669179fc6967884db69c17186cb8fc
96f2de9b0ac5922ab53c595df1e3513bb3f2642b458d96e3782dbb975a8b4faed":"830f178cf5f544140d2d8c0737790b
97bc6f150784865548d73f1f37a5a39a65":"cb12a2b9a02aaaeae4c7c76cad9e006186d978bc046c1ea81532bc51601ed
e00":"2d3dde3b3581b863e1590bdc638c33bfd170555445e225f3a450d9e9762abec1":"fddf7f1b906861d49da9660e7
716b5ef987163e7e2f51f4fef2cb3e8d01b736067765aaea11a7d193266b2e0071e4d4c8cc776399464563adb9deae22b
d721ed03b148516100b9f340a00d2632c80c5b3e1f93825ffeb112fb90e658d638740e62d8031fabfe40f79c20532e667
aeacc6be635f64a0580236d7d978c5db017c76a6767dc419ba2f89102a88e53254f41205866e875225380ae04943bcc8f
152c9fd79a680557d1f2a0a8ac7b27900bba33db63e26e0d7363034af1430b6546a3ce2c01c8cfe0e152f106baa5b2fae1
fe00cef10154b735fdfae354ececc7da44c914b054cd97d99866a9d5df42765cd62eaf1b8adc885fa2263911c837b4643f
"
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 7 (0x7)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=NL, O=PolarSSL, CN=PolarSSL Test CA
    Validity
      Not Before: Feb 12 14:44:07 2011 GMT
      Not After : Feb 12 14:44:07 2021 GMT
    Subject: C=NL, O=PolarSSL, CN=PolarSSL Cert SHA1
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (2048 bit)
        Modulus (2048 bit):
          00:b9:3c:4a:c5:c8:a3:8e:90:17:a4:9e:52:aa:71:
          75:26:61:80:e7:c7:b5:6d:8c:ff:aa:b6:41:26:b7:
          be:11:ad:5c:73:16:0c:64:11:48:04:ff:d6:e1:3b:
          05:db:89:bb:b3:97:09:d5:1c:14:dd:68:87:39:b0:
          3d:71:cb:e2:76:d0:1a:d8:18:2d:80:1b:54:f6:e5:
          44:9a:f1:cb:af:61:2e:df:49:0d:9d:09:b7:ed:b1:
          fd:3c:fd:3c:fa:24:cf:5d:bf:7c:e4:53:e7:25:b5:
          ea:44:22:e9:26:d3:ea:20:94:9e:e6:61:67:ba:2e:
          07:67:0b:03:2f:a2:09:ed:f0:33:8f:0b:ce:10:ef:
          67:a4:c6:08:da:c1:ed:c2:3f:d7:4a:dd:15:3d:f9:
          5e:1c:81:60:46:3e:b5:b3:3d:2f:a6:de:47:1c:bc:

92:ae:eb:df:27:6b:16:56:b7:dc:ec:d1:55:57:a5:
6e:ec:75:25:f5:b7:7b:df:ab:d2:3a:5a:91:98:7d:
97:17:0b:13:0a:a7:6b:4a:8b:c1:47:30:fb:3a:f8:
41:04:d5:c1:df:b8:1d:bf:7b:01:a5:65:a2:e0:1e:
36:b7:a6:5c:cc:30:5a:f8:cd:6f:cd:f1:19:62:25:
ca:01:e3:35:7f:fa:20:f5:dc:fd:69:b2:6a:00:7d:
17:f7
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
X509v3 Subject Key Identifier:
7D:E4:9C:6B:E6:F9:71:7D:46:D2:12:3D:AD:6B:1D:FD:C2:AA:78:4C
X509v3 Authority Key Identifier:
keyid:B4:5A:E4:A5:B3:DE:D2:52:F6:B9:D5:A6:95:0F:EB:3E:BC:C7:FD:FF

Signature Algorithm: sha1WithRSAEncryption
93:26:40:68:3d:e7:62:ea:d1:6a:78:2b:c2:07:f3:0d:3b:f6:
69:18:cd:08:5e:31:e7:48:60:08:2a:46:b6:de:d1:35:0a:ec:
31:36:83:7d:eb:7c:d8:63:09:c3:e4:c5:10:ca:7c:7b:2f:20:
4d:d2:0e:5f:ee:09:e3:84:4f:28:cc:08:74:9a:11:23:5f:de:
0e:3a:0f:8b:2d:64:91:05:f6:d5:c7:30:c8:20:ee:6c:c4:62:
7c:8d:a8:4d:2e:70:8c:ac:b5:5d:de:9b:10:5c:98:fd:a1:78:
9b:9c:f0:73:33:de:2f:8c:59:fa:dc:af:4c:df:97:e3:9d:00:
37:9a:fa:d3:67:77:b9:2f:b9:4a:23:ad:f9:b4:a1:b7:ac:c5:
a8:0f:62:8c:e6:7e:b4:94:2a:db:f2:fc:52:92:a4:9e:4e:51:
4f:9d:c0:ce:ae:3d:17:1c:94:6c:5f:e8:16:b5:ce:2e:e2:5a:
cf:6a:db:dd:b0:d4:be:62:a5:46:92:30:7c:7c:fc:05:f8:78:
30:93:30:28:ab:69:a1:72:31:dc:3b:97:63:3a:5b:b3:e1:34:
86:80:4a:28:f5:dc:d5:84:8c:13:a4:6c:d2:c1:2d:a6:25:d7:
6f:c9:93:78:a5:16:ba:d9:17:6e:3e:ca:96:f2:9e:5c:e3:ae:
12:2e:a5:11
-----BEGIN
CERTIFICATE-----
MIIDQDCCAiigAwIBAgIBBzANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTEwMjEyMTQ0NDA3WhcNMjEwMjEyMTQ0NDA3WjA9MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxGzAZBgNVBAMTElBvbGFyU1NMIENlcnQgU0hBMTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALk8SsXIo46QF6SeUqpxdSZhgOfH
tW2M/6q2QSa3vhGtXHMWDGQRSAT/1uE7BduJu7OXCdUcFN1ohzmwPXHL4nbQGtgY
LYAbVPblRJrxy69hLt9JDZ0Jt+2x/Tz9POkz12/fORT5yW16kQi6SbT6iCUnuZh
Z7ouB2cLAy+iCe3wM48LzhDvZ6TGCNrB7cI/10rdFT35XhyBYEY+tbM9L6beRxy8
kq7r3ydrFla33OzRVVelbux1JfW3e9+r0jpakZh9lxcLEwqna0qLwUcw+zr4QQTV
wd+4Hb97AaVlouAeNremXMwwWvjNb83xGWIlygHjNX/6IPXc/WmyagB9F/cCAwEA
AaNNMEswCQYDVR0TBAIwADAdBgNVHQ4EFgQUfeSca+b5cX1G0hI9rWsd/cKqeEww
HwYDVR0jBBgwFoAUtFrkpbPe0lL2udWmlQ/rPrzH/f8wDQYJKoZIhvcNAQEFBQAD
ggEBAJMmQGg952Lq0Wp4K8IH8w079mkYzQheMedIYAgqRrbe0TUK7DE2g33rfNhj
CcPkxRDKfHsvIE3SDl/uCeOETyjMCHSaESNf3g46D4stZJEF9tXHMMgg7mzEYnyN

qE0ucIystV3emxBcmP2heJuc8HMz3i+MWfrcr0zfl+OdADea+tNnd7kvuUojrfm0
obesxagPYozmfrSUKtvy/FKSpJ5OUU+dwM6uPRcclGxf6Ba1zi7iWs9q292w1L5i
pUaSMHx8/AX4eDCTMCiraaFyMdw7l2M6W7PhNIaASij13NWEjBOkbNLBLaYl12/J
k3ilFrrZF24+ypbynlzjrhIupRE=
-----END
CERTIFICATE-----
Client_identity:6162636465666768696a6b6c6d6e6f70
-----BEGIN CERTIFICATE-----
MIIDWzCCAhKgAwIBAgIBGDA+BgkqhkiG9w0BAQowMaANMAsGCWCGSAFlAwQCAaEa
MBgGCSqGSIb3DQEBCDALBglghkgBZQMEAgSiBAICAN4wOzELMAkGA1UEBhMCTkwx
ETAPBgNVBAoTCFBvbGFyU1NMMRkwFwYDVQQDExBQb2xhclNTTCBUZXN0IENBMB4X
DTE0MDEyMDEzNTc0NVoXDTI0MDExODEzNTc0NVowNDELMAkGA1UEBhMCTkwxETAP
BgNVBAoTCFBvbGFyU1NMMRIwEAYDVQQDEwlsb2NhbGhvc3QwgZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBAN0Rip+ZurBoyirqO2ptWZftTslU5A3uzqB9oB6q6A7C
uxNA24oSjokTJKXF9frY9ZDXyMrLxf6THa/aEiNzUnlGGrqgVyt2FjGzqK/nOJsI
i2OZOgol7kXSGFi6uZMa7dRYmmMbN/z3FAifhWVJ81kybdHg6G3eUu1mtKkL2kCV
AgMBAAGjgZIwgY8wCQYDVR0TBAIwADAdBgNVHQ4EFgQU7vPH9R8VpU1HicHTImOy
36fOvVEwYwYDVR0jBFwwWoAUtFrkpbPe0lL2udWmlQ/rPrzH/f+hP6Q9MDsxCzAJ
BgNVBAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEZMBcGA1UEAxMQUG9sYXJTU0wg
VGVzdCBDQYIBADA+BgkqhkiG9w0BAQowMaANMAsGCWCGSAFlAwQCAaEaMBgGCSqG
SIb3DQEBCDALBglghkgBZQMEAgSiBAICAN4DggEBAIfliohNjz4CLGbHWgWRBFQ3
Difn027ZnULTvokT67ii1sJzESzqaIakyyu8GRwfoFRNh/rbGfe4C6e9SkwKbnDg
WE9SWbK6ukIQbMy69C+CVqFlRUHbONw/dmcneAWyZYGx/2Sf4D5kkpIWNDBeKuaV
H69XPZCeN3QAACmdAfo4NYW0I69a1OSaUrTyGT1nBOrzQ8Y0aJBnCJAte49bhQEW
KJv0kMj+8ZG1X0RoSdklf3GqdLUbsfJ2txu14GGAxy4C1gl2JWzoBHN5LMLf0cZ9
uEYui7N/5bkSv8KXdbGvSzgn6zZ0MiCJMiiGEf0L1FxBiBCVsK4C2idpiZH+e28=
-----END
CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,B5FA3F70C2AF79EB9D3DD2C40E7AE61A

iyfOvvyTPPR7on4XPFxu6CoCgTqh88ROlslM+RLJhwM/qGexbgDOzeI2CPf4XfzI
tyevKD/pqCaCMesYJh/HDQCILdW2tGbwzPajg72xkfCD6+1NHOGoDbdQN8ahGVmg
flAYU0iXDMvqs/jnucM7nlTGp8Istn7+zd9ARyrkQy+I8nvMh3chGKWzx/XtJR+z
Iv8p+n/o+fCHzGvtj+LWYeUc4d0OTIjnF6QPTtPOexX28z0gXRODT/indgifNXv3
j45KO2NYOaVTaCuiWIHj7wWBokoL4bCMFcFTJbdJx5BgfLmDkTEmB/6DEXu6UOsQ
3lPzyJhIRxn7hNq2I47TzSAFvmcXwm84txpxtSwHTcl9LgsyIiEMmHv3lPPE1G94
F5VrCzzFHyU7nFRdUC0mqLrCHcjDn5O4SQWfH7J/7G4OArU6lA4Z2NC03IPxEmsQ
66Fu8GdMbmtFORdlZQtOjLi3zZwN9+NwhiUrNNdVvGNJIjIcZ4FZRZysbt7++hfQ
/JOAKhVNC8dNROJUleEYIiqx23e5lze6wqcIosziq3tb6/SQ6fH533D8+PpcZKsC
IlWKAQzsNV+nJvt7CI1ppWc6CtV7TKn0scZm2oOC4339gdR5xzxXe9EJDsMBpcg9
drIdBr+3UxeC6Lc/rWM7IjSQ2YULBra3toEF6UYevngXdUD2YafrpoY5rK9IH90G
Hjbf65IaHLTS0jA7lAvJsQEBuULQQoWENOjhp8v+UfkNM2ccyOuUk3xZJNeX19YP
1Z09UMEKbf6ucoRCc01SBl206OAsq1NZEaodszT+mDg990I/9ACVi3LEU6XB5ZVs
-----END RSA PRIVATE KEY-----
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"

```
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
   <Configuration>Release</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\pkey\rsa_encrypt.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">
    <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid>{D06CF12E-F222-9273-41BF-B8A052FA5527}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>rsa_encrypt</RootNamespace>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
```

```
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
/>
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
   <PrecompiledHeader>
```

```
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
     <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
   </Link>
   <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
   </ProjectReference>
  </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
   <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
   <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
   </Link>
   <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
   </ProjectReference>
  </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
```

<IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
<AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
</ClCompile>
<Link>
<SubSystem>Console</SubSystem>
<GenerateDebugInformation>true</GenerateDebugInformation>
<EnableCOMDATFolding>true</EnableCOMDATFolding>
<OptimizeReferences>true</OptimizeReferences>
<AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
</Link>
</ItemDefinitionGroup>
<ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
<ClCompile>
<WarningLevel>Level3</WarningLevel>
<PrecompiledHeader>
</PrecompiledHeader>
<Optimization>MaxSpeed</Optimization>
<FunctionLevelLinking>true</FunctionLevelLinking>
<IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
<AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
</ClCompile>
<Link>
<SubSystem>Console</SubSystem>
<GenerateDebugInformation>true</GenerateDebugInformation>
<EnableCOMDATFolding>true</EnableCOMDATFolding>
<OptimizeReferences>true</OptimizeReferences>
<AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
</Link>
</ItemDefinitionGroup>
<Import
Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
<ImportGroup Label="ExtensionTargets">
</ImportGroup>
</Project>
-----BEGIN X509 CRL-----
MIIBqzCBlDANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDERMA8GA1UEChMI
UG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EXDTExMDIyMDEwMjI1
OVoXDTE5MTEyNTEwMjI1OVowKDASAgEBFw0xMTAyMTIxNDQ0MDdaMBICAQMXDTEx
MDIxMjE0NDQwN1owDQYJKoZIhvcNAQEFBQADggEBAJYuWdKPdblMVWCnxpMnchuL
dqWzK2BA0RelCaGjpxuwX3NmLDm+5hKja/DJxaRqTOf4RSC3kcX8CdIldsLO96dz
//wAQdFPDhy6AFT5vKTO8ItPHDb7qFOqFqpeJi5XN1yoZGTB1ei0mgD3xBaKbp6U
yCOZJSIFomt7piT4GcgWVHLUmpyHDDeodNhYPrN0jf2mr+ECd9fQJYdz1qm0Xx+Q

NbKXDiPRmPX0qVleCZSeSp1JAmU4GoCO+96qQUpjgll+6xWya3UNj61f9sh0Zzr7
5ug2LZo5uBM/LpNR1K3TLxNCcg7uUPTn9r143d7ivJhPl3tEJn4PXjv6mlLoOgU=
-----END X509 CRL-----
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIGRMBwGCiqGSIb3DQEMAQEwDgQIIrlmCCSpJzcCAggABHGm2LyJ60ojfilRRp8h
Xf+sWL3lJq6wlj4Nk41SHVnZ2RiVtP5NVK908/WxnXkridd6Qpjnq/14woWVmQxT
IzhKFVi22YmQyBsNj+bEGDAE4c9qaby8u6zbzs7Qj29F90f/PiYsaIEGcNn/W88e
XarNDw==
-----END ENCRYPTED PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDBTCCAeegAwIBAgIBFjATBgkqhkiG9w0BAQowBqIEAgIA6jA7MQswCQYDVQQG
EwJOTDERMA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3Qg
Q0EwHhcNMTQwMTIwMTMzODE2WhcNMjQwMTE4MTMzODE2WjA0MQswCQYDVQQGEwJO
TDERMA8GA1UEChMIUG9sYXJTU0wxEjAQBgNVBAMTCWxvY2FsaG9zdDCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA3RGKn5m6sGjKKuo7am1Zl+1OyVTkDe7OoH2g
HqroDsK7E0DbihKOiRMkpcX1+tj1kNfIysvF/pMdr9oSI3NSeUYauqBXK3YWMbOo
r+c4mwiLY5k6CiXuRdIYWLq5kxrt1FiaYxs3/PcUCJ+FZUnzWTJt0eDobd5S7Wa0
qQvaQJUCAwEAAaOBkjCBjzAJBgNVHRMEAjAAMB0GA1UdDgQWBBTu88f1HxWlTUeJ
wdMiY7Lfp869UTBjBgNVHSMEXDBagBS0WuSls97SUva51aaVD+s+vMf9/6E/pD0w
OzELMAkGA1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NMMRkwFwYDVQQDExBQb2xh
clNTTCBUZXN0IENBggEAMBMGCSqGSIb3DQEBCjAGogQCAgDqA4IBAQDAog/jXydR
vDIugTzBXtfVK0CEX8iyQ4cVzQmXWSne8204v943K5D2hktSBkjdQUdcnVvVgLR6
te50jV89ptN/NofX+fo9fhSRN9vGgQVWzOOFiO0zcThy749pirJu1Kq5OJdthIyW
Pu0UCz5G0k3kTp0JPevGlsNc8S9Ak1tFuB0IPJjrbfODWHS2LDuO+dB6gpkNTdrj
88ogYtBsN4D5gsXBRUfobXokUwejBwLrD6XwyQx+0bMwSCxgHEhxvuUkx1vdlXGw
JG3aF92u8mIxoKSAPaPdqy930mQvmpUWcN5Y1IMbtEGoQCKMYgosFcazJpJcjnX1
o4Hl/lqjwCFG
-----END
CERTIFICATE-----
P =
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514
A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E
9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A
163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED52907709696
6D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C
55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AACAA68FFFFFFF
FFFFFFFFF
G = 02
test_suites
The various 'test_suite_XXX' programs from the 'tests' directory, executed using 'make check' (Unix make) or 'make test' (Cmake), include test cases (reference test vectors, sanity checks, malformed input for parsing functions, etc.) for all modules except the SSL modules.

selftests
The 'programs/test/selftest' program runs the 'XXX_self_test()' functions of each individual module. Most of them are included in the respective test suite, but some slower ones are only included here.

compat
  The 'tests/compat.sh' script checks interoperability with OpenSSL and
  GnuTLS (and ourselves!) for every common ciphersuite, in every TLS
  version, both ways (client/server), using client authentication or not.
  For each ciphersuite/version/side/authmode it performs a full handshake
  and a small data exchange.

ssl_opt
  The 'tests/ssl-opt.sh' script checks various options and/or operations not
  covered by compat.sh: session resumption (using
 session cache or tickets),
  renegotiation, SNI, other extensions, etc.
-----BEGIN CERTIFICATE-----
MIIBzDCCAVOgAwIBAgIJAPOkPR3wsvm5MAoGCCqGSM49BAMCMD4xCzAJBgNVBAYT
Ak5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBF
QyBDQTAeFw0xNDA0MDkxMTI0MTNaFw0yNDA0MDYxMTI0MTNaMD4xCzAJBgNVBAYT
Ak5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBF
QyBDQTB2MBAGByqGSM49AgEGBSuBBAAiA2IABMPaKzRBN1gvh1b+/Im6KUNLTuBu
ww5XUzM5WNRStJGVOQsj318XJGJI/BqVKc4sLYfCiFKAr9ZqqyHduNMcbli4yuiy
aY7zQa0pw7RfdadHb9UZKVVpmlM7ILRmFmAzHqMdMBswDAYDVR0TBAUwAwEB/zAL
BgNVHQ8EBAMCB4AwCgYIKoZIzj0EAwIDZwAwZAIwGRCmU/rWNjW13g8ITuq3pMXb
jgwTFJHVlbMDiFJwUrRvytPV9doJOfzJ8nAQ0cZ1AjAbJ8QAV2e+DmYZpWc/p6Ug
nQdac59ev+lH+ju6wET3jNDjUthUPrdgqa54+UWQ5r4=
-----END CERTIFICATE-----
-----BEGIN EC PARAMETERS-----
BggqhkjOPQMBBw==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIP3MTs0m9ssAAXQ94O6GYC3pckfpMUxQiPTG8hQYgA0WoAoGCCqGSM49
AwEHoUQDQgAEBHU9DhX+RlHK4F9l5ZQsicz/eDWeOuBrIAeqbDS7A3i/o+wFPqCc
u1S71v5R4dzg4JdPGfW4aixQZjY5x25vEA==
-----END EC PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIICHzCCAaWgAwIBAgIBFDAKBggqhkjOPQQDAzA+MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EwHhcN
MTMwOTI0MTYyMTI3WhcNMjMwOTIyMTYyMTI3WjA0MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxEjAQBgNVBAMTCWxvY2FsaG9zdDBZMBMGByqGSM49AgEG
CCqGSM49AwEHA0IABDfMVtl2CR5acj7HWS3/IG7ufPkGkXTQrRS192giWWKSTuUA
2CMR/+ov0jRdXRa9iojCa3cNVc2KKg76Aci07f+jgZ0wgZowCQYDVR0TBAIwADAd
BgNVHQ4EFgQUUGGlj9QH2deCAQzlZX+MY0anE74wbgYDVR0jBGcwZYAUnW0gJEkB
PyvLeLUZvH4kydv7NnyhQqRAMD4xCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQb2xh
clNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBFQyBDQYIJAMFD4n5iQ8zoMAoG
CCqGSM49BAMDA2gAMGUCMQCnsd/6VB2kLIqMRsWdkJvRaQROyAg78CQExFEY3CMv
9t0kWRXPc4nCMH69RjQVvC4CMB4lk9A7hnX2zQy3bbUhOCOvXcsQdEe8AMgJBviz
5Nob2wThRqsm1wjCF60fyzXWuA==
-----END CERTIFICATE-----

```
-----BEGIN EC PRIVATE KEY-----
MIHcAgEBBEIBsbatB7t55zINpZhg6ijgVShPYFjyed5mbgbUNdKve9oo2Z+ke33Q
lj4WsAcweO6LijjZZqWC9G0Z/5XfOtloWq6gBwYFK4EEACOhgYkDgYYABAAd4ULV
T2nrA47kt6+dPKB3Nv2c9xnrNU1ph57n88E2+w+/nwj4a+X6Eo7BoFHT5sZD6Fra
j/rPNmPCYL0shEtvVgDO6OSKnmXQnK3YnyNd7gXzuKZGvnFfH2fVtDTg/yOh/Afv
d0AZPkDu/287zf12WqkVUDNST+TyBfVETiksTC9qwQ==
-----END EC PRIVATE KEY-----
set(libs
  mbedtls
)

if(USE_PKCS11_HELPER_LIBRARY)
  set(libs ${libs} pkcs11-helper)
endif(USE_PKCS11_HELPER_LIBRARY)

if(ENABLE_ZLIB_SUPPORT)
  set(libs ${libs} ${ZLIB_LIBRARIES})
endif(ENABLE_ZLIB_SUPPORT)

add_executable(cert_app cert_app.c)
target_link_libraries(cert_app ${libs})

add_executable(crl_app crl_app.c)
target_link_libraries(crl_app ${libs})

add_executable(req_app req_app.c)
target_link_libraries(req_app ${libs})

add_executable(cert_req cert_req.c)
target_link_libraries(cert_req ${libs})

add_executable(cert_write cert_write.c)
target_link_libraries(cert_write ${libs})

install(TARGETS cert_app crl_app req_app cert_req cert_write
    DESTINATION "bin"
    PERMISSIONS OWNER_READ OWNER_WRITE OWNER_EXECUTE GROUP_READ
GROUP_EXECUTE WORLD_READ WORLD_EXECUTE)
language: c
compiler:
- clang
- gcc
sudo: false
cache: ccache
script:
- tests/scripts/recursion.pl library/*.c
- tests/scripts/check-generated-files.sh
- tests/scripts/check-doxy-blocks.pl
```

```
- tests/scripts/check-names.sh
- tests/scripts/doxygen.sh
- cmake -D CMAKE_BUILD_TYPE:String="Check" .
- make
- make test
- programs/test/selftest
- OSSL_NO_DTLS=1 tests/compat.sh
- tests/ssl-opt.sh -e '\(DTLS\|SCSV\).*openssl'
- tests/scripts/test-ref-configs.pl
- tests/scripts/curves.pl
- tests/scripts/key-exchanges.pl
after_failure:
- tests/scripts/travis-log-failure.sh
env:
 global:
   secure:
"barHldniAfXyoWOD/vcO+E6/Xm4fmcaUoC9BeKW+LwsHqlDMLvugaJnmLXkSpkbYhVL61Hzf3bo0KPJn88A
Fc5Rkf8oYHPjH4adMnVXkf3B9ghHCgznqHsAH3choo6tnPxaFgOwOYmLGb382nQxfE5lUdvnM/W/psQjWt66
A1+k="

addons:
 apt:
   packages:
   - doxygen
   - graphviz
 coverity_scan:
   project:
     name: "ARMmbed/mbedtls"
   notification_email: p.j.bakker@polarssl.org
   build_command_prepend:
   build_command: make
   branch_pattern:
 coverity_scan
Certificate:
   Data:
       Version: 3 (0x2)
       Serial Number: 8 (0x8)
       Signature Algorithm: sha224WithRSAEncryption
       Issuer: C=NL, O=PolarSSL, CN=PolarSSL Test CA
       Validity
           Not Before: Feb 12 14:44:07 2011 GMT
           Not After : Feb 12 14:44:07 2021 GMT
       Subject: C=NL, O=PolarSSL, CN=PolarSSL Cert SHA224
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
           RSA Public Key: (2048 bit)
               Modulus (2048 bit):
                   00:b9:3c:4a:c5:c8:a3:8e:90:17:a4:9e:52:aa:71:
```

75:26:61:80:e7:c7:b5:6d:8c:ff:aa:b6:41:26:b7:
be:11:ad:5c:73:16:0c:64:11:48:04:ff:d6:e1:3b:
05:db:89:bb:b3:97:09:d5:1c:14:dd:68:87:39:b0:
3d:71:cb:e2:76:d0:1a:d8:18:2d:80:1b:54:f6:e5:
44:9a:f1:cb:af:61:2e:df:49:0d:9d:09:b7:ed:b1:
fd:3c:fd:3c:fa:24:cf:5d:bf:7c:e4:53:e7:25:b5:
ea:44:22:e9:26:d3:ea:20:94:9e:e6:61:67:ba:2e:
07:67:0b:03:2f:a2:09:ed:f0:33:8f:0b:ce:10:ef:
67:a4:c6:08:da:c1:ed:c2:3f:d7:4a:dd:15:3d:f9:
5e:1c:81:60:46:3e:b5:b3:3d:2f:a6:de:47:1c:bc:
92:ae:eb:df:27:6b:16:56:b7:dc:ec:d1:55:57:a5:
6e:ec:75:25:f5:b7:7b:df:ab:d2:3a:5a:91:98:7d:
97:17:0b:13:0a:a7:6b:4a:8b:c1:47:30:fb:3a:f8:
41:04:d5:c1:df:b8:1d:bf:7b:01:a5:65:a2:e0:1e:
36:b7:a6:5c:cc:30:5a:f8:cd:6f:cd:f1:19:62:25:
ca:01:e3:35:7f:fa:20:f5:dc:fd:69:b2:6a:00:7d:
17:f7
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
X509v3 Subject Key Identifier:
7D:E4:9C:6B:E6:F9:71:7D:46:D2:12:3D:AD:6B:1D:FD:C2:AA:78:4C
X509v3 Authority Key Identifier:
keyid:B4:5A:E4:A5:B3:DE:D2:52:F6:B9:D5:A6:95:0F:EB:3E:BC:C7:FD:FF

Signature Algorithm: sha224WithRSAEncryption
b8:9b:0a:d1:b4:d1:a4:ce:05:39:42:7a:3b:7b:5e:fd:97:57:
8a:36:60:42:39:d0:e6:0c:9c:7e:2f:2b:be:ef:e7:45:34:77:
48:7a:10:4a:fd:76:ca:42:39:25:3c:fa:19:f8:63:6c:e7:36:
27:9a:ec:06:ce:e4:f7:2c:2e:c6:36:c1:25:bd:ab:09:aa:e2:
da:4e:de:ae:b5:f5:ba:9e:90:24:52:34:96:96:61:4c:26:b5:
57:65:b1:10:ed:13:2b:54:90:ce:d3:21:cb:8c:d3:4c:6c:e5:
e1:78:22:16:3f:e1:be:f1:ee:5d:39:48:a1:e6:80:46:f4:46:
f2:79:03:3e:f1:fc:51:47:d9:05:e8:85:81:1b:0b:4f:fa:85:
9d:ce:e7:76:5a:6f:da:98:9f:43:f1:f3:2f:2f:57:28:aa:70:
14:82:7f:d5:69:14:8c:f9:82:b6:2f:a6:df:b5:6b:0e:43:c9:
96:91:64:3d:8b:a8:17:15:9a:88:42:a4:d0:90:c0:a3:a2:e1:
dd:f6:95:6d:3b:9d:71:a6:1e:9e:2c:1e:db:f6:5f:93:43:2c:
ed:53:70:55:50:56:df:cd:96:6c:d5:91:0f:b1:a7:f4:b7:17:
9d:1f:0b:f6:0b:f8:fe:e7:7c:de:c1:20:b7:fc:69:13:ba:e2:
61:9b:a5:62
-----BEGIN
CERTIFICATE-----
MIIDQjCCAiqgAwIBAgIBCDANBgkqhkiG9w0BAQ4FADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTEwMjEyMTQ0NDA3WhcNMjEwMjEyMTQ0NDA3WjA/MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxHTAbBgNVBAMTFFBvbGFyU1NMIENlcnQgU0hBMjI0MIIB

IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuTxKxcijjpAXpJ5SqnF1JmGA
58e1bYz/qrZBJre+Ea1ccxYMZBFIBP/W4TsF24m7s5cJ1RwU3WiHObA9ccvidtAa
2BgtgBtU9uVEmvHLr2Eu30kNnQm37bH9PP08+iTPXb985FPnJbXqRCLpJtPqIJSe
5mFnui4HZwsDL6IJ7fAzjwvOEO9npMYI2sHtwj/XSt0VPfleHIFgRj61sz0vpt5H
HLySruvfJ2sWVrfc7NFVV6Vu7HUl9bd736vSOlqRmH2XFwsTCqdrSovBRzD7OvhB
BNXB37gdv3sBpWWi4B42t6ZczDBa+M1vzfEZYiXKAeM1f/og9dz9abJqAH0X9wID
AQABo00wSzAJBgNVHRMEAjAAMB0GA1UdDgQWBBR95Jxr5vlxfUbSEj2tax39wqp4
TDAfBgNVHSMEGDAWgBS0WuSls97SUva51aaVD+s+vMf9/zANBgkqhkiG9w0BAQ4F
AAOCAQEAuJsK0bTRpM4FOUJ6O3te/ZdXijZgQjnQ5gycfi8rvu/nRTR3SHoQSv12
ykI5JTz6GfhjbOc2J5rsBs7k9ywuxjbBJb2rCari2k7errX1up6QJFI0lpZhTCa1
V2WxEO0TK1SQztMhy4zTTGzl4XgiFj/hvvHuXTlIoeaARvRG8nkDPvH8UUfZBeiF
gRsLT/qFnc7ndlpv2pifQ/HzLy9XKKpwFIJ/1WkUjPmCti+m37VrDkPJlpFkPYuo
FxWaiEKk0JDAo6Lh3faVbTudcaYeniwe2/Zfk0Ms7VNwVVBW382WbNWRD7Gn9LcX
nR8L9gv4/ud83sEgt/xpE7riYZulYg==
-----END
CERTIFICATE-----
-----BEGIN EC PARAMETERS-----
BggqhkjOPQMBBw==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIAiUS1dM3qrcOun8PjKe+rw40L2HG/Y8Dfxl0AfzyIVeoAoGCCqGSM49
AwEHoUQDQgAEayEqtszvZg9vWAixweehXVP0SDbUYX3i7TPruaNx2gJ6KctEvfEc
7hBhC46c6/GSOpJDDGbI/JxWUBfB37hNIA==
-----END EC PRIVATE KEY-----
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 5 (0x5)
    Signature Algorithm: md4WithRSAEncryption
    Issuer: C=NL, O=PolarSSL, CN=PolarSSL Test CA
    Validity
      Not Before: Feb 12 14:44:07 2011 GMT
      Not After : Feb 12 14:44:07 2021 GMT
    Subject: C=NL, O=PolarSSL, CN=PolarSSL Cert MD4
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (2048 bit)
        Modulus (2048 bit):
          00:b9:3c:4a:c5:c8:a3:8e:90:17:a4:9e:52:aa:71:
          75:26:61:80:e7:c7:b5:6d:8c:ff:aa:b6:41:26:b7:
          be:11:ad:5c:73:16:0c:64:11:48:04:ff:d6:e1:3b:
          05:db:89:bb:b3:97:09:d5:1c:14:dd:68:87:39:b0:
          3d:71:cb:e2:76:d0:1a:d8:18:2d:80:1b:54:f6:e5:
          44:9a:f1:cb:af:61:2e:df:49:0d:9d:09:b7:ed:b1:
          fd:3c:fd:3c:fa:24:cf:5d:bf:7c:e4:53:e7:25:b5:
          ea:44:22:e9:26:d3:ea:20:94:9e:e6:61:67:ba:2e:
          07:67:0b:03:2f:a2:09:ed:f0:33:8f:0b:ce:10:ef:
          67:a4:c6:08:da:c1:ed:c2:3f:d7:4a:dd:15:3d:f9:

```
            5e:1c:81:60:46:3e:b5:b3:3d:2f:a6:de:47:1c:bc:
            92:ae:eb:df:27:6b:16:56:b7:dc:ec:d1:55:57:a5:
            6e:ec:75:25:f5:b7:7b:df:ab:d2:3a:5a:91:98:7d:
            97:17:0b:13:0a:a7:6b:4a:8b:c1:47:30:fb:3a:f8:
            41:04:d5:c1:df:b8:1d:bf:7b:01:a5:65:a2:e0:1e:
            36:b7:a6:5c:cc:30:5a:f8:cd:6f:cd:f1:19:62:25:
            ca:01:e3:35:7f:fa:20:f5:dc:fd:69:b2:6a:00:7d:
            17:f7
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints:
        CA:FALSE
      X509v3 Subject Key Identifier:
        7D:E4:9C:6B:E6:F9:71:7D:46:D2:12:3D:AD:6B:1D:FD:C2:AA:78:4C
      X509v3 Authority Key Identifier:
        keyid:B4:5A:E4:A5:B3:DE:D2:52:F6:B9:D5:A6:95:0F:EB:3E:BC:C7:FD:FF

  Signature Algorithm: md4WithRSAEncryption
    94:db:e1:86:71:2d:43:d6:51:61:a7:95:bc:e8:73:da:ff:e4:
    fd:41:0f:5c:de:14:f4:c4:ba:5d:2c:30:2c:a6:dc:2d:e8:87:
    45:f1:c5:fe:d1:4a:64:99:19:09:2f:72:7c:3f:8d:c8:31:22:
    dd:0a:69:03:3d:12:8c:4d:c3:f7:a3:c5:d1:5d:c9:ff:4b:83:
    6b:d6:b4:e5:d8:ce:94:5e:ec:bf:68:c5:b2:63:8e:5c:cb:f3:
    8d:62:73:82:62:7e:df:db:7d:0b:8d:21:10:db:9a:a1:62:4d:
    46:42:d1:bb:38:32:ef:c1:fc:a1:e2:7f:60:08:37:32:20:2c:
    7c:a2:c9:12:0d:89:fe:2b:15:08:91:79:e2:a9:79:a4:da:cd:
    81:43:01:e2:09:2d:1a:f4:16:ef:af:4d:50:46:5e:2d:dd:48:
    27:10:c0:42:b7:a5:9e:c2:1f:6e:50:36:03:ed:95:77:9a:a3:
    d9:4c:d7:23:93:b1:24:2a:63:27:28:7a:de:3d:59:d2:92:c8:
    8f:f6:39:1d:65:ab:09:78:05:46:90:a9:f6:10:b1:ef:c8:8c:
    4d:7d:8d:f2:78:b7:88:15:09:7e:df:e9:87:a8:64:c1:95:53:
    fb:da:05:b7:62:bc:ad:fb:d9:a4:a9:06:6c:6b:98:01:b9:39:
    78:d3:4e:87
-----BEGIN CERTIFICATE-----
MIIDPzCCAiegAwIBAgIBBTANBgkqhkiG9w0BAQMFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTEwMjEyMTQ0NDA3WhcNMjEwMjEyMTQ0NDA3WjA8MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxGjAYBgNVBAMTEVBvbGFyU1NMIENlcnQgTUQ0MIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuTxKxcijjpAXpJ5SqnF1JmGA58e1
bYz/qrZBJre+Ea1ccxYMZBFIBP/W4TsF24m7s5cJ1RwU3WiHObA9ccvidtAa2Bgt
gBtU9uVEmvHLr2Eu30kNnQm37bH9PP08+iTPXb985FPnJbXqRCLpJtPqIJSe5mFn
ui4HZwsDL6IJ7fAzjwvOEO9npMYI2sHtwj/XSt0VPfleHIFgRj61sz0vpt5HHLyS
ruvfJ2sWVrfc7NFVV6Vu7HUl9bd736vSOlqRmH2XFwsTCqdrSovBRzD7OvhBBNXB
37gdv3sBpWWi4B42t6ZczDBa+M1vzfEZYiXKAeM1f/og9dz9abJqAH0X9wIDAQAB
o00wSzAJBgNVHRMEAjAAMB0GA1UdDgQWBBR95Jxr5vlxfUbSEj2tax39wqp4TDAf
BgNVHSMEGDAWgBS0WuSls97SUva51aaVD+s+vMf9/zANBgkqhkiG9w0BAQMFAAOC
AQEAlNvhhnEtQ9ZRYaeVvOhz2v/k/UEPXN4U9MS6XSwwLKbcLeiHRfHF/tFKZJkZ
CS9yfD+NyDEi3QppAz0SjE3D96PF0V3J/0uDa9a05djOlF7sv2jFsmOOXMvzjWJz
```

gmJ+39t9C40hENuaoWJNRkLRuzgy78H8oeJ/YAg3MiAsfKLJEg2J/isVCJF54ql5
pNrNgUMB4gktGvQW769NUEZeLd1IJxDAQrelnsIfblA2A+2Vd5qj2UzXI5OxJCpj
Jyh63j1Z0pLIj/Y5HWWrCXgFRpCp9hCx78iMTX2N8ni3iBUJft/ph6hkwZVT+9oF
t2K8rfvZpKkGbGuYAbk5eNNOhw==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDPzCCAiegAwIBAgIBATANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTEwMjEyMTQ0NDA2WhcNMjEwMjEyMTQ0NDA2WjA8MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxGjAYBgNVBAMTEVBvbGFyU1NMIFNlcnZlciAxMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqQIfPUBq1VVTi/027oJlLhVhXom/
uOhFkNvuiBZS0/FDUEeWEllkh2v9K+BG+XO+3c+S4ZFb7Wagb4kpeUWA0INq1UFD
d185fAkER4KwVzlw7aPsFRkeqDMIR8EFQqn9TMO0390GH00QUUBncxMPQPhtgSVf
CrFTxjB+FTms+Vruf5KepgVb5xOXhbUjktnUJAbVCSWJdQfdphqPPwkZvq1lLGTr
lZvc/kFeF6babFtpzAK6FCwWJJxK3M3Q91Jnc/EtoCP9fvQxyi1wyokLBNsupk9w
bp7OvViJ4lNZnm5akmXiiD8MlBmj3eXonZUT7Snbq3AS3FrKaxerUoJUsQIDAQAB
o00wSzAJBgNVHRMEAjAAMB0GA1UdDgQWBBQfdNY/KcF0dEU7BRIsPai9Q1kCpjAf
BgNVHSMEGDAWgBS0WuSls97SUva51aaVD+s+vMf9/zANBgkqhkiG9w0BAQUFAAOC
AQEAvc+WwZUemsJu2IiI2Cp6liA+UAvIx98dQe3kZs2zAoF9VwQbXcYzWQ/BILkj
NImKbPL9x0g2jIDn4ZvGYFywMwIO/d++YbwYiQw42/v7RiMy94zBPnzeHi86dy/0
jpOOJUx3IXRsGLdyjb/1T11klcFqGnARiK+8VYolMPP6afKvLXX7K4kiUpsFQhUp
E5VeM5pV1Mci2ETOJau2cO40FJvI/C9W/wR+GAArMaw2fxG77E3laaa0LAOlexM6
A4KOb5f5cGTM5Ih6tEF5FVq3/9vzNIYMa1FqzacBLZF8zSHYLEimXBdzjBoN4qDU
/WzRyYRBRjAI49mzHX6raleqnw==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTcwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTgwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASsc/JkNcYf
bMgpOfrL5kKOGxOJaGS6SQIeNO33UeBpToe1bU2acN652xjvcGo0fJEtxg2fcPHR
hTnGMBD1u1N2o4GJMIGGMB0GA1UdDgQWBBSDbIpYntlhJ0GgIsyd75XRhlC18jBX
BgNVHSMEUDBOgBSnjWvpWxZcFnfQ2KGtCg/u6fT/D6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTE2ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAJo2NXfJU1sK6SVTu4OV21FKITlXntMi
oenYMsBjzO8oAiEAidSELcLjjAHi3mfBARvCgKlRhmbNEMCHQT7Ha7ZQoRw=
-----END CERTIFICATE-----
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">

```
    <Configuration>Debug</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
    <Configuration>Release</Configuration>
    <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
    <Configuration>Release</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\pkey\key_app_writer.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">
     <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid>{E8ED79F9-8034-1B09-263E-D3F8C4C5C4A8}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>key_app_writer</RootNamespace>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
```

```
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')"
 Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup
 Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
   <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <LinkIncremental>false</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
   <LinkIncremental>false</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <ClCompile>
     <PrecompiledHeader>
     </PrecompiledHeader>
     <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>

<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
```

```
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
```

```
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
   </Link>
 </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
   <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
   <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
   </Link>
 </ItemDefinitionGroup>
  <Import Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
-----BEGIN CERTIFICATE-----
MIIBpTCCAUugAwIBAgIJAPygloXKk6BwMAoGCCqGSM49BAMCMC8xCzAJBgNVBAYT
AlVLMREwDwYDVQQKDAhtYmVkIFRMUzENMAsGA1UEAwwEQ0EwMDAeFw0xNzA2MjIx
MTUwMzJaFw0yNzA2MjMxMTUwMzJaMC8xCzAJBgNVBAYTAlVLMREwDwYDVQQKDAht
YmVkIFRMUzENMAsGA1UEAwwEQ0EwMDBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IA
BFW41/qAwAPpy+Txdc7PKmzZsq9CPiujKU4vpF1ekXnGx2HP420QobwBVVWhkzRm
LwdboH2j65dcCKjQ7mv/dxKjUDBOMB0GA1UdDgQWBBQlFYvU5WboI4fcdPoiQs8/
fPHZrTAfBgNVHSMEGDAWgBQlFYvU5WboI4fcdPoiQs8/fPHZrTAMBgNVHRMEBTAD
AQH/MAoGCCqGSM49BAMCA0gAMEUCIQC7iRcVzwMyfVK5imirJ7MqJQ04euH4CLOt
IZ+SNfaERAIgSU0MWFDosVEIpg8YMqIHeF7Mg4ZyH6+fGazJgVLttUY=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIC6jCCAnCgAwIBAgIBCDAKBggqhkjOPQQDAjA+MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EwHhcN
```

MTMwOTI0MTU1MjA0WhcNMjMwOTIyMTU1MjA0WjA0MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxEjAQBgNVBAMTCWxvY2FsaG9zdDCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBAKvXjL5VfYc7D/truqEpYcZcvlUhnuCNDJctYDJL
vgYYj5uxDxLHBXvnEHLgO5K+lps42p+r/dd4oE64ttRoeZZUvr+7eBnW35n0EpPA
Ik9Gwu+vg7GfxmifgIR8hZnOQkt2OjvvpChPCxvUailtB450Izh+mEK/hYFr+7Jl
NnxR1XQlbbyDM7Ect1HwYcuS3MBlBqq048J+0KEkQXICSjKeHFga9eDCq+Jyfqe5
bt0K30hl1N0164B7aoh08Eomme+aSuAsz+MsJ3m7AO2DUYdrDxlrky1QrvRWWfX0
d8djTM+uHTo1DviRM6o9+P9DfoFd53/Z0Km03sVLQWvUrhECAwEAAaOBnTCBmjAJ
BgNVHRMEAjAAMB0GA1UdDgQWBBTAlAm1+0L41mhqYWjFiejsRVrGeTBuBgNVHSME
ZzBlgBSdbSAkSQE/K8t4tRm8fiTJ2/s2fKFCpEAwPjELMAkGA1UEBhMCTkwxETAP
BgNVBAoTCFBvbGFyU1NMMRwwGgYDVQQDExNQb2xhcnNzbCBUZXN0IEVDIENBggkA
wUPifmJDzOgwCgYIKoZIzj0EAwIDaAAwZQIxAPWlxnMcjBaxaVieQYSLBqzizS3/
O8Na6owRGPk0/UK+j5O9NTBHk+uXW/fQblKamQIwUQl4dl6gkRDE4rBR/yGjZZ1Z
3dEpvL2Wimt3keD7AcLpYB2FJ1mVcY1XQUeK1Vfc
-----END
CERTIFICATE-----
XTEA Encrypt_ecb #1
xtea_encrypt_ecb:"000102030405060708090a0b0c0d0e0f":"4142434445464748":"497df3d072612cb5"

XTEA Encrypt_ecb #2
xtea_encrypt_ecb:"000102030405060708090a0b0c0d0e0f":"4141414141414141":"e78f2d13744341d8"

XTEA Encrypt_ecb #3
xtea_encrypt_ecb:"000102030405060708090a0b0c0d0e0f":"5a5b6e278948d77f":"4141414141414141"

XTEA Encrypt_ecb #4
xtea_encrypt_ecb:"00000000000000000000000000000000":"4142434445464748":"a0390589f8b8efa5"

XTEA Encrypt_ecb #5
xtea_encrypt_ecb:"00000000000000000000000000000000":"4141414141414141":"ed23375a821a8c2d"

XTEA Encrypt_ecb #6
xtea_encrypt_ecb:"00000000000000000000000000000000":"70e1225d6e4e7655":"4141414141414141"

XTEA Decrypt_ecb #1
xtea_decrypt_ecb:"000102030405060708090a0b0c0d0e0f":"497df3d072612cb5":"4142434445464748"

XTEA Decrypt_ecb #2
xtea_decrypt_ecb:"000102030405060708090a0b0c0d0e0f":"e78f2d13744341d8":"4141414141414141"

XTEA Decrypt_ecb #3
xtea_decrypt_ecb:"000102030405060708090a0b0c0d0e0f":"4141414141414141":"5a5b6e278948d77f"

XTEA
Decrypt_ecb #4
xtea_decrypt_ecb:"00000000000000000000000000000000":"a0390589f8b8efa5":"4142434445464748"

XTEA Decrypt_ecb #5

xtea_decrypt_ecb:"00000000000000000000000000000000":"ed23375a821a8c2d":"4141414141414141"

XTEA Decrypt_ecb #6
xtea_decrypt_ecb:"00000000000000000000000000000000":"4141414141414141":"70e1225d6e4e7655"

XTEA Encrypt CBC #1
xtea_encrypt_cbc:"000102030405060708090a0b0c0d0e0f":"6162636465666768":"4142434445464748":"6b982bec15a7b558"

XTEA Encrypt CBC #2
xtea_encrypt_cbc:"000102030405060708090a0b0c0d0e0f":"4142434445464748":"41414141414141414141414141414141":"2c6aeb799561c8e973b0927f072e3801"

XTEA Encrypt CBC #3
xtea_encrypt_cbc:"000102030405060708090a0b0c0d0e0f":"0000000000000000":"5a5b6e278948d77f70e1225d6e4e7655e78f2d13744341d8":"41414141414141415fee100fe2c030025d8a557f2677cb33"

XTEA Encrypt CBC #4
xtea_encrypt_cbc:"00000000000000000000000000000000":"6162636465666768":"4142434445464748":"5b0c065a3803900d"

XTEA Encrypt CBC #5
xtea_encrypt_cbc:"00000000000000000000000000000000":"4142434445464748":"41414141414141414141414141414141":"bdae508aa320aa5caa7cd79dbc9c38aa"

XTEA
Encrypt CBC #6
xtea_encrypt_cbc:"00000000000000000000000000000000":"0000000000000000":"5a5b6e278948d77f70e1225d6e4e7655e78f2d13744341d8":"61f5082a2c996f632da3ea16ff8e06558b69f069d8637b31"

XTEA Decrypt CBC #1
xtea_decrypt_cbc:"000102030405060708090a0b0c0d0e0f":"6162636465666768":"4142434445464748":"359def46515c71b2"

XTEA Decrypt CBC #2
xtea_decrypt_cbc:"000102030405060708090a0b0c0d0e0f":"4142434445464748":"41414141414141414141414141414141":"1b192d63cc0e90371b1a2f66c809963e"

XTEA Decrypt CBC #3
xtea_decrypt_cbc:"000102030405060708090a0b0c0d0e0f":"0000000000000000":"5a5b6e278948d77f70e1225d6e4e7655e78f2d13744341d8":"2e76e5cc03543cdc40ca03358a5764c331a0631c2f0f3714"

XTEA Decrypt CBC #4
xtea_decrypt_cbc:"00000000000000000000000000000000":"6162636465666768":"4142434445464748":"81476a15138174dc"

XTEA Decrypt CBC #5
xtea_decrypt_cbc:"00000000000000000000000000000000":"4142434445464748":"41414141414141414141414141414141

1414141":"31a361192b08311d31a0631c2f0f3714"

XTEA
Decrypt CBC #6
xtea_decrypt_cbc:"00000000000000000000000000000000":"0000000000000000":"5a5b6e278948d77f70e1225d6e
4e7655e78f2d13744341d8":"c1e2dbbf67ee786e29e051bea18c6abc66f1de5c2daefc2a"

XTEA Selftest
depends_on:MBEDTLS_SELF_TEST
xtea_selftest:
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTUwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTYwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQ7Vsp7JmDN
kgPh/+zmIPkd7o0xot/WPMFn3uAsGtsU385MF0fmhfFLhRbbH9h4JjYHj8y0spU3
buUXhftvAZVbo4GJMIGGMB0GA1UdDgQWBBRTw3K0Psy3u/6+3KKSoaQqJnPvPjBX
BgNVHSMEUDBOgBR1mXlrdW5rx1VnqMMnUBXo0WWGWqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTE0ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAMJnGjE9v3SjuGfi0jNByrwyNfhlTHMh
FhPQidNrDpXwAiEAqYtNiV8t9RrAa9GC6FWDuJpvIiU6FsE+lFq6uIq/J2E=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTQwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTUwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQlKUiMoSss
/hsTasedqdB2BCOGJhTt0hgUGeUnWNZ1svO4yn0GkFHZ08++fl2MKqjpj+VXq0JS
FFyGUOgmgi3Ho4GJMIGGMB0GA1UdDgQWBBR1mXlrdW5rx1VnqMMnUBXo0WWGWjBX
BgNVHSMEUDBOgBRNsJB++ccSBmbCCKBxi4CjXROBk6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTEzggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAKYOIo+fdCQRqpH4LN8qUK1aKzKmWGxS
fGzEEkg/29bMAiAl95cmucoCDMq2Ab8Coc0dEqyJ6+rAPMLBCbGawyiW6A==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTMwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTQwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATRMZN0RHzP
donNmZuq9XPhzvQ52TaokxT39qpQtlFyvUuEGKrLoNvdcpARaA0rGput6RLAQOVU
iNVlJ3Ipj789o4GJMIGGMB0GA1UdDgQWBBRNsJB++ccSBmbCCKBxi4CjXROBkzBX
BgNVHSMEUDBOgBTmVnUSF2MYwws/nCMv7b1wJVkDmqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTEyggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgVfuLpjp08AaxKWf6cuZUUCRd7CojSS1I
71hzeUyFS+sCIQDNJI6P/pBbiHgTaGlBAgfcEfmxmbY0n4xZndtxIkmyVA==
-----END

CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTIwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTMwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATrkzCJLznh
lhnsv1RXB9kfeaD+cIruPQ0cItBDGpdvD8xbBVvQci4+RG2RVUCSWRhkFYjSsUSM
0QHMQnBFlhw2o4GJMIGGMB0GA1UdDgQWBBTmVnUSF2MYwws/nCMv7b1wJVkDmjBX
BgNVHSMEUDBOgBTZTtbi+j0Sm/Zs/+gTkWdASpQzfqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTExggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgWsm+rHJgwUEyNm8EKbEds5yurpp5/3y5
PsvXJVDqxogCIQDUP0Jcl3A907CE2tPVXSgD6LQ6CPu19mixemPw60yijA==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTEwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTIwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATDE9LPlLPc
gZ3b0BchR/AkhNEP9HAavwYadJIyzoPo5edCVnboQH786jsZwZNZoC0gHDAhCmGc
IfRenISAoVuPo4GJMIGGMB0GA1UdDgQWBBTZTtbi+j0Sm/Zs/+gTkWdASpQzfjBX
BgNVHSMEUDBOgBSOSt6ePyMRT6PGMaIi7FqNX9MKtKEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTEwggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgYYF5AnRV7eh2hLD5Dz//pceMTKz9Ls46
E6DxvbfDHikCIFttlGrOCZVyS4ocsjuKIELVUX5qfygI0sn4kU3qCTs2
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTAwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATZwR+WK6NB
F/7riFdN63c8hjYddZRR4lrzVNPwiBQxnnxwpPyrD9A6aPPmLc6SqGOJW4ZGVCco
IBze9RJVeiB9o4GJMIGGMB0GA1UdDgQWBBSOSt6ePyMRT6PGMaIi7FqNX9MKtDBX
BgNVHSMEUDBOgBQtxZSLJAkEz+2RKMQexM6EtsfgcqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA5ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgN//NqM0FrkrMjmxoeCY9DgxkH2R6sQ4d
NgtwCZAIqEICIBs4vupaVcuvni9tltbP26wi7c0FR+blZuo5DPIA3SVe
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDkwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTAwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAR6jlGKbJd5
hiDxN789gkOcwpyHI9wRwCrADAOwOkMePBPRlwGdm7mw7Z/EAmu26zRm/hcyrs4M
qk2LabDjPI9Xo4GJMIGGMB0GA1UdDgQWBBQtxZSLJAkEz+2RKMQexM6EtsfgcjBX
BgNVHSMEUDBOgBT6gyXHzPIPYc1Vr1aGiLLeMh4HpqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA4ggEBMAwGA1UdEwQF

MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgP7S8vFstfUBdNe6ym5GYG5Q+aBVEKqRs
fVW7HNUktSYCIQDo6Jua6o/DJbrpq4qYWq5gv4yGyzPTN+3IaKrEICdaaw==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDgwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDkwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAR7ZB16+t6E
sfahGyKUGJW5mezkzjdaYvc4lbJaKNRwFRfc3F/fmNOSsUFSg/F0N+vUE+doKiPC
8wRwLzvm4s+5o4GJMIGGMB0GA1UdDgQWBBT6gyXHzPIPYc1Vr1aGiLLeMh4HpjBX
BgNVHSMEUDBOgBS40mLt93U8Sh8ZGiDVAhRSiBPcXqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA3ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgO4el1ZPhlIli/qNR2SIEiuvs5Mmy868i
N2Rv5X/VxIECIA/8rUALQxW38XSdBVX3e/jzu7ju47n1YwEqD9K9WdVv
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDcwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDgwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAARpQeQ/YGQj
nl7Szo6WStJ1u7xunTL5jBkXH8aAVSm0qiX4AD/7YPxa5EnGzZdLTn25vQVnfQAG
pMx8P1lYiGYCo4GJMIGGMB0GA1UdDgQWBBS40mLt93U8Sh8ZGiDVAhRSiBPcXjBX
BgNVHSMEUDBOgBREq5J3toJPxZ3O+ssJ5vkkU0RJE6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA2ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhANwGf+F4a+kmXWz8UjSpRkaToTV6EFWw
/Tjzj0tQhDoAAiEA19RxeWOVBBpM6LOHg6v5Lf54YN1snkLf+sEXyZCuWQQ=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDYwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDcwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASNOj4d4MEA
7p/3miijqG4ToE4opKPAm+3BTIGrJTYT14++TSiUICl0ASXj+xeUcLMIaXTN042s
LsHxpShzQaL0o4GJMIGGMB0GA1UdDgQWBBREq5J3toJPxZ3O+ssJ5vkkU0RJEzBX
BgNVHSMEUDBOgBSjovYaC/m6Li9Tp0V9iZRs9267Q6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA1ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAKGcf+c442c/XiwubbaiQvsoZ7EoVxuM
oKmia0gPyBNkAiEA83asjJ5FDXQuLyZpczviXrbmqgCPOfYadtvkc0cxMis=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDUwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDYwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASA9qWoAUHr
nn+3kxyNrjPJk82WDLimW21RN51uxpobadv8YgGEDRdP+Ok+uRqQSUsA6ZXfF3iG
r2GjfQ3wMDH8o4GJMIGGMB0GA1UdDgQWBBSjovYaC/m6Li9Tp0V9iZRs9267QzBX

BgNVHSMEUDBOgBTXh06MAV9S4l4lG1TKOrKRBh4qn6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA0ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgcjZNFWJtlDmoPZbAxqsGczRYK0lfPgu6
g1H7pp0ce+wCIDj9BRZM2OB9EF0e+MDKGjyZGfvfrL6Ir47x/KrM6H8T
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDQwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDUwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQEdT0OFf5G
UcrgX2XllCyJzP94NZ464GsgB6psNLsDeL+j7AU+oJy7VLvW/lHh3ODgl08Z9bhq
LFBmNjnHbm8Qo4GJMIGGMB0GA1UdDgQWBBTXh06MAV9S4l4lG1TKOrKRBh4qnzBX
BgNVHSMEUDBOgBQox4F1NsZunlsduoGvzIgRSYfB36EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAzggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAIW++zqDZlLLUk/emePohdNOp5JO3wS9
XvkBJ6Wua7GBAiAdx+EKmdjVrwnzrQltTgnmSfGMXhKNYifK3uD83W3pcQ==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDMwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDQwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQUXDgcUVNT
9hovbZE5HL6rjOb7C55wEuWKThV/CcZ4rWrXx7VXHYdD/R3aDA7JSvYpm2sTok4i
sblDzhZM/GDNo4GJMIGGMB0GA1UdDgQWBBQox4F1NsZunlsduoGvzIgRSYfB3zBX
BgNVHSMEUDBOgBQApzZdtBdD3dLxouQpr/aDiVttd6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAyggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgAkiNhqFAZXSUWEDK91OZvQGdeZOtd6mC
+Wv3fGk3t28CIEKOwidkUTUaiPdZ4efmAr+CEeGzdq27ob2S+nqqHqgV
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDIwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDMwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQRDXDNIi1p
ereudhqwa2LslXgsxnB63Hu5y5lg+1WPruIYPzD/Ho0APveVdzFLVji19+bE4+tF
PYL1SpsN1WfWo4GJMIGGMB0GA1UdDgQWBBQApzZdtBdD3dLxouQpr/aDiVttdzBX
BgNVHSMEUDBOgBT5RCgQ0AlZTQbfFB2+6+w0XRvydaEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAxggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAOnd+7bAofkHVa4KFNjv3TCegw1lrhuM
8Of8wgvrTEGoAiEAsS8iKMpSfXH4D0egg4gLamE6akde965rDtySU+ve9lg=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDEwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx

DTALBgNVBAMMBENBMDIwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQWHpv1i6lf
wvNPOP5ka6S0n55EvzoaYK6pbTXP6yMOW/4XZSPKx5Zoq4FMe0cKzGIIFL1rzj1V
2czYB+qvLhyio4GJMIGGMB0GA1UdDgQWBBT5RCgQ0AlZTQbfFB2+6+w0XRvydTBX
BgNVHSMEUDBOgBSh3uHkX5nj86yFEFwjscSWM40P+qEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAI7unGW/gr9tOc3i+dF5N815srgh+FrX
oj9Et74EcSpTAiBubv+vOH0DE0gmYI11HeAIgutWqqMIC72dZlwTF/Vi3g==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB3jCCAYWgAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDAwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQznn9zHHwL
GO8VR4W9V7vMlxCdoojzEOiX5Y6JtPtFOz866ueHY6zoN0/mJ6DnqnSXilJIUUeW
6eGfqmka7nxko4GRMIGOMB0GA1UdDgQWBBSh3uHkX5nj86yFEFwjscSWM40P+jBf
BgNVHSMEWDBWgBQlFYvU5WboI4fcdPoiQs8/fPHZraEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggkA/KCWhcqToHAw
DAYDVR0TBAUwAwEB/zAKBggqhkjOPQQDAgNHADBEAiBasbuinP+pJTU4oDCVD8zQ
1rJBDSOKIEyWu84/D6Hj6wIgVMPUoO01bPhzllAa/gW8Xk/daey09SBgN3AT9pWU
TDA=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIBpTCCAUugAwIBAgIJAPygloXKk6BwMAoGCCqGSM49BAMCMC8xCzAJBgNVBAYT
AlVLMREwDwYDVQQKDAhtYmVkIFRMUzENMAsGA1UEAwwEQ0EwMDAeFw0xNzA2MjIx
MTUwMzJaFw0yNzA2MjMxMTUwMzJaMC8xCzAJBgNVBAYTAlVLMREwDwYDVQQKDAht
YmVkIFRMUzENMAsGA1UEAwwEQ0EwMDBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IA
BFW41/qAwAPpy+Txdc7PKmzZsq9CPiujKU4vpF1ekXnGx2HP420QobwBVVWhkzRm
LwdboH2j65dcCKjQ7mv/dxKjUDBOMB0GA1UdDgQWBBQlFYvU5WboI4fcdPoiQs8/
fPHZrTAfBgNVHSMEGDAWgBQlFYvU5WboI4fcdPoiQs8/fPHZrTAMBgNVHRMEBTAD
AQH/MAoGCCqGSM49BAMCA0gAMEUCIQC7iRcVzwMyfVK5imirJ7MqJQ04euH4CLOt
IZ+SNfaERAIgSU0MWFDosVEIpg8YMqIHeF7Mg4ZyH6+fGazJgVLttUY=
-----END CERTIFICATE-----
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIE4zAcBgoqhkiG9w0BDAEBMA4ECCLhzdwnOXIZAgIIAASCBMG8Wgfn++CFRl37
FdQZ90pI+u37yj8v0kFd3rDaDMurEftf10gWwTbm8R8J0eK1edIAHQabkgsF83gD
yrxKFp1zhHI1t65gPKHcirhx0t9XuClxAOzEme//iMaw/yf/IKYo9NRqyvA6BKHW
2h3J4+JSGLSaCsRUyzhoL6xOzF+VX8zE8PI11TcqfJe7TGs/9G0Pv2XxFpfrG7pz
nz5mkAYdckYHcu7+CQGJ09ZUkblV3MYKEEbq5xXEo4Kku/n1YNrh6BEWMLo5XgOU
YIAkzhSfnbTt6QrxM+90b4qwk5amrC4w1jUu73ZzaBQs7fhx01pR2y3zTPBD2Dpk
G3iLprgEFqsoGCCOqqqEiEF/xDREZEPW0es2RruQ9Tn14LbgTj5XVFI/wBcvp9uZ
pjS5chC0/CRbGcRi47A9vx9bjgwiGCDpxx0/Kn68uFCaCeGOAQ687XxAn1UHmBD3
esjjb7S16ld9rSKV0oXWugUZKFdoq87AHY8Njhin++biuAEfySu3iH5ajzZV9dEj
6JHVwotuL2diVu7NU8mIsfr1kCJoUxIAbWFvoglWNmTtaIBkc5ch+kUTsz9rDtSp
lL9fT+wzjN7Q7lyRfIhNOheg2xF9huwF6mqnSlDfvwvEJ8NsQI9+CeooI2c1Zc0a
Bh/vDvCzov8TE+1Ma8CnrbaM/aSZ0FIq6PcpWSBLXSDXbLwabEEOLoXQXogOZsc5
0sz71l5c8jJPlzXxFYYW8CNuxTsUP+hN2oWvbmL5YLq8P+1tw68jcdbqhTqoqrW1

pGEXd2iMRUfCTDuCM6Bn4iIN80qUqqBAuoTC+zCVHnI7+ygmovhf/ykfVzNaDSIW
BkDsmZoH6bq3F9HpvOWggh0yK/l1b1E4PDQ6hq7qWNyJMyjYBJEbEdd9O3GW2qev
3ARhb0yGulxYH/h3yp2mIfxL+UTfRMcUZD2SobL+phLR/9TMUi6IaHnBAF85snAb
rbtAKCp9myFLwG1BujaQ18fKQFgcMjbJY3gLIz+3AC72irLSdgGti2drjP2hDGKp
RITAEydZXIwf67JMKkvyuknVWMf9ri9tMOZEvohnU3bW4g9vkv89CUtCLWF8iejM
fKIP5hjHOcKRLvvACFbgjYCPt8iPCcQckYe+FZI5T7zYsyQQ47fygS1f7MWZblPJ
UKAm8jxWUyySvEzIMHkoZaHtC72OS/L3iCjJ7mkKSZKeCDAzSEJeeQcOl0klVCQ8
0P+mXq5wtGakW9MKLhmsOjUIsyN2f3gCO0nESYhWD+3EKFLSW7ZsHbDmwqSDh6bn
blFvlQd7cpfYFtlmbxZFcv/l2ijQWPHi93G/0VIhFHxI6LegKt00bIL5iwyF3NpW
dNzuE69hweTSKvOPqRsRnWyGv9dVLIaQPwUS+eEfsGGNzM9rbty0j5Bw6KY/uDgt
blTfN3yZBcyEsdPwyiVLdi65zMzN8g4VVQBHFhXWPa2N4gJQVq+6q9hQkgFFU7y3
f8MX4BrKq8ifwWxsjL2FawcAoDcHUdCZjt/HZ+9/rL3iQvKeHbDbqu4kxlrE1FJn
0LHIB21qZIo+6r3fdNMUFkuDRBT9eEh3Wxlg8G35FYCIiOuIwB2ED/Hdnqtnemxj
kjRXU176HQ==
-----END
ENCRYPTED PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDFTCCAf0CDFOittkjXbxFc/m3bDANBgkqhkiG9w0BAQsFADBOMRowGAYDVQQD
ExFzZXJ2ZXIxL2ludC1jYS12MTEQMA4GA1UECxMHdGVzdGluZzERMA8GA1UEChMI
UG9sYXJTU0wxCzAJBgNVBAYTAk5MMCIYDzIwMTQwNjE5MTAwOTI5WhgPMjAyNDA2
MTgxMDA5MjlaMEQxEDAOBgNVBAMTB3NlcnZlcjIxEDAOBgNVBAsTB3Rlc3Rpbmcx
ETAPBgNVBAoTCFBvbGFyU1NMMQswCQYDVQQGEwJOTDCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBAMFNo93nzR3RBNdJcriZrA545Do8Ss86ExbQWuTNowCI
p+4ea5anUrSQ7y1yej4kmvy2NKwk9XfgJmSMnLAofaHa6ozmyRyWvP7BBFKzNtSj
+uGxdtiQwWG0ZlI2oiZTqqt0Xgd9GYLbKtgfoNkNHC1JZvdbJXNG6AuKT2kMtQCQ
4dqCEGZ9rlQri2V5kaHiYcPNQEkI7mgM8YuG0ka/0LiqEQMef1aoGh5EGA8PhYva
i0Re4hjGYi/HZo36Xdh98yeJKQHFkA4/J/EwyEoO79bex8cna8cFPXrEAjyaHT4P
6DSYW8tzS1KW2BGiLICIaTla0w+w3lkvEcf36hIBMJcCAwEAATANBgkqhkiG9w0B
AQsFAAOCAQEAivCCMBfC5YNeozwp8vAWpiRUakhtO8ysvCfQsZD4tWLlSkrjoUtG
3RNd9gDVDGb852GswtNMKHJC1AeZuXdh3eBoDBNTXnR/9UkHgWNBy5f+JH2irYrc
ps5ofpYJZe7K6xQjl+RLc8nfUUaVfS3dJnyLr9k5kg4in48p+hEF6oXDBu2zdufF
53k/U98FTvFkVisEDFzLXyKX0fAZxfMk4qnEoBflH4fEXfkuuaBUVdoGGIMRLNAW
GIyRxr+zj+OJL+ZjjAkY4JqtEuUuLjODn//DHI/MkqE0LANOvbb4akpgZsyvSSO3
o38d1wQHw5+bO+YDqdfIdQXguU5mtS1xAw==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDITCCAgkCDFOitscEzU2OvIALwTANBgkqhkiG9w0BAQsFADBQMRwwGgYDVQQD
ExNQb2xhclNTTCBUZXN0IENBIHYxMRAwDgYDVQQLEwd0ZXN0aW5nMREwDwYDVQQK
EwhQb2xhclNTTDELMAkGA1UEBhMCTkwwIhgPMjAxNDA2MTkxMDA5MTFaGA8yMDI0
MDYxODEwMDkxMVowTjEaMBgGA1UEAxMRc2VydmVyMS9pbnQtY2EtdjExEDAOBgNV
BAsTB3Rlc3RpbmcxETAPBgNVBAoTCFBvbGFyU1NMMQswCQYDVQQGEwJOTDCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKkCHz1AatVVU4v9Nu6CZS4VYV6J
v7joRZDb7ogWUtPxQ1BHlhJZZIdr/SvgRvlzvt3PkuGRW+1moG+JKXlFgNCDatVB
Q3dfOXwJBEeCsFc5cO2j7BUZHqgzCEfBBUKp/UzDtN/dBh9NEFFAZ3MTD0D4bYEl
XwqxU8YwfhU5rPla7n+SnqYFW+cTl4W1I5LZ1CQG1QkliXUH3aYajz8JGb6tZSxk
65Wb3P5BXhem2mxbacwCuhQsFiScStzN0PdSZ3PxLaAj/X70McotcMqJCwTbLqZP
cG6ezr1YieJTWZ5uWpJl4og/DJQZo93l6J2VE+0p26twEtxaymsXq1KCVLECAwEA

ATANBgkqhkiG9w0BAQsFAAOCAQEAPJl3fbVeTJ6gVAvCoLYM8JY5U7ZhrCCdBghw
WuZBS/TWwf4WLP0G/ZtTyTOENcT0gWHf0/VnXtNPw2/yBjWsLtTXxN2XQlEVf3j/
WcQxWgSESYdx/sT/uTW6qihuONPWkTQizmx7OG6vBuGx3g54s9/oeJKXOraNqud3
G4KBrytOazliMfoKO2hnzaeydpaDtb2tZX8apN/6KqQpTAcXsWrZRW9XEHWq2sNz
IR1nIE1F/9gnqi9Xy0HQprteLRUvM4tEQ35m4H20eS5Y9gJlE/DqXmMQ7aiU8DgP
krj+Z18pcrssO+Etv0BOiPjmU9TWWpDMj34ef7U/OH5qJxkSrA==
-----END
CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDdEYqfmbqwaMoq6jtqbVmX7U7JVOQN7s6gfaAequgOwrsTQNuK
Eo6JEySlxfX62PWQ18jKy8X+kx2v2hIjc1J5Rhq6oFcrdhYxs6iv5zibCItjmToK
Je5F0hhYurmTGu3UWJpjGzf89xQIn4VlSfNZMm3R4Oht3lLtZrSpC9pAlQIDAQAB
AoGAHFCE2tBL0xB45Go/1e/Pi9//OVZAJ3Cw0mmEuqjVNB7I6zxhYhviWbgz92+V
g92KBlU9CIx0/ZhGMyHRNO0uYNEZUJyM8zItoo/nmU31+VaHOGgpei04HZrn1Nmw
QS01FVrn9wzKR/5qeEBmxE7rVMDQo8QLnllC3jXzIVUtX4ECQQD2g9dleWYbqIQe
Q9paXxzvODhCzNtQwD0PnOKc54Nu4zm3JI45REtunmG8et+Ncms9RycTjNlWPGJT
62jgaJexAkEA5ZMNv4u9NNRfZprmlNyvjSOf+w7fdKzhcnkHbGkfLnFdc7vq0XFC
nwORsdjpOvWQUwrV2Cw8Pl4rKa4B4iqUJQJBAMVti6maU3udN8qhXxP3js3LwctG
E/OVMpH5fMha5jl9w/B4V2tn1d3O/MmdwsKeu2JFRPd0W2+kRr+dDs6DFdECQQC1
3g9QJRWY2n1RPXlZiJKSDxzXuOqQ9bwMAZE98vE+y5Qq8T2O+li6vAsZhysNCChz
gOvzuudmyRcMh8r6Lpz5AkAUKK3gYtJFiVH2arRig3JjZJqixgSTolMT1n+HG4uM
tnBqBiEBVwBxEqaohla/rHR5joZCdcDN8xq0yeTQyLH9
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIB7DCCAXOgAwIBAgIBPTAKBggqhkjOPQQDAjA+MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EwHhcN
MTQwNDEwMTcyMTQyWhcNMjQwNDA3MTcyMTQyWjA0MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxEjAQBgNVBAMTCWxvY2FsaG9zdDBZMBMGByqGSM49AgEG
CCqGSM49AwEHA0IABDfMVtl2CR5acj7HWS3/IG7ufPkGkXTQrRS192giWWKSTuUA
2CMR/+ov0jRdXRa9iojCa3cNVc2KKg76Aci07f+jbDBqMAkGA1UdEwQCMAAwHQYD
VR0OBBYEFFBhpY/UB9nXggEM5WV/jGNGpxO+MB8GA1UdIwQYMBaAFJ1tICRJAT8r
y3i1Gbx+JMnb+zZ8MB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAKBggq
hkjOPQQDAgNnADBkAjAmQjJxxC82ZhBpH/GQkOQXDmaaV/JHRHGok1cWn3j3Xj8A
fqRZkp8JihpGIMse208CMFCMdNAfNd1tv+oPuynoK5Oh6/YlASX/otJT68voEIAN
SmsT1m9VPQMIyUo/3RtYjg==
-----END CERTIFICATE-----
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
<ItemGroup Label="ProjectConfigurations">
<ProjectConfiguration Include="Debug|Win32">
<Configuration>Debug</Configuration>
<Platform>Win32</Platform>
</ProjectConfiguration>
<ProjectConfiguration Include="Debug|x64">
<Configuration>Debug</Configuration>
<Platform>x64</Platform>
</ProjectConfiguration>

```
  <ProjectConfiguration Include="Release|Win32">
    <Configuration>Release</Configuration>
    <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
    <Configuration>Release</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
</ItemGroup>
<ItemGroup>
  <ClCompile Include="..\..\programs\x509\crl_app.c" />
</ItemGroup>
<ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">

 <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
</ItemGroup>
<PropertyGroup Label="Globals">
  <ProjectGuid>{DB904B85-AD31-B7FB-114F-88760CC485F2}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>crl_app</RootNamespace>
</PropertyGroup>
<Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
</PropertyGroup>
<Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
```

```
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
 />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
    <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
   <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <LinkIncremental>false</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
   <LinkIncremental>false</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <ClCompile>
     <PrecompiledHeader>
     </PrecompiledHeader>
     <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
      <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
     <SubSystem>Console</SubSystem>
     <GenerateDebugInformation>true</GenerateDebugInformation>
```

```
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
```

```
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
   </Link>
 </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
   <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
   <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
   </Link>
 </ItemDefinitionGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.targets"
 />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
Certificate:
   Data:
      Version: 3 (0x2)
      Serial Number: 0 (0x0)
      Signature Algorithm: sha1WithRSAEncryption
      Issuer: C=NL, O=PolarSSL, CN=PolarSSL Test CA
      Validity
         Not Before: Feb 12 14:44:00 2011 GMT
         Not After : Feb 12 14:44:00 2021 GMT
      Subject: C=NL, O=PolarSSL, CN=PolarSSL Test CA
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
         RSA Public Key: (2048 bit)
            Modulus (2048 bit):
               00:c0:df:37:fc:17:bb:e0:96:9d:3f:86:de:96:32:
               7d:44:a5:16:a0:cd:21:f1:99:d4:ec:ea:cb:7c:18:
               58:08:94:a5:ec:9b:c5:8b:df:1a:1e:99:38:99:87:
```

```
                1e:7b:c0:8d:39:df:38:5d:70:78:07:d3:9e:d9:93:
                e8:b9:72:51:c5:ce:a3:30:52:a9:f2:e7:40:70:14:
                cb:44:a2:72:0b:c2:e5:40:f9:3e:e5:a6:0e:b3:f9:
                ec:4a:63:c0:b8:29:00:74:9c:57:3b:a8:a5:04:90:
                71:f1:bd:83:d9:3f:d6:a5:e2:3c:2a:8f:ef:27:60:
                c3:c6:9f:cb:ba:ec:60:7d:b7:e6:84:32:be:4f:fb:
                58:26:22:03:5b:d4:b4:d5:fb:f5:e3:96:2e:70:c0:
                e4:2e:bd:fc:2e:ee:e2:41:55:c0:34:2e:7d:24:72:
                69:cb:47:b1:14:40:83:7d:67:f4:86:f6:31:ab:f1:
                79:a4:b2:b5:2e:12:f9:84:17:f0:62:6f:27:3e:13:
                58:b1:54:0d:21:9a:73:37:a1:30:cf:6f:92:dc:f6:
                e9:fc:ac:db:2e:28:d1:7e:02:4b:23:a0:15:f2:38:
                65:64:09:ea:0c:6e:8e:1b:17:a0:71:c8:b3:9b:c9:
                ab:e9:c3:f2:cf:87:96:8f:80:02:32:9e:99:58:6f:
                a2:d5
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:TRUE
            X509v3 Subject Key Identifier:
                B4:5A:E4:A5:B3:DE:D2:52:F6:B9:D5:A6:95:0F:EB:3E:BC:C7:FD:FF
            X509v3 Authority Key Identifier:
                keyid:B4:5A:E4:A5:B3:DE:D2:52:F6:B9:D5:A6:95:0F:EB:3E:BC:C7:FD:FF
                 DirName:/C=NL/O=PolarSSL/CN=PolarSSL Test CA
                serial:00

    Signature Algorithm: sha1WithRSAEncryption
        b8:fd:54:d8:00:54:90:8b:25:b0:27:dd:95:cd:a2:f7:84:07:
        1d:87:89:4a:c4:78:11:d8:07:b5:d7:22:50:8e:48:eb:62:7a:
        32:89:be:63:47:53:ff:b6:be:f1:2e:8c:54:c0:99:3f:a0:b9:
        37:23:72:5f:0d:46:59:8f:d8:47:cd:97:4c:9f:07:0c:12:62:
        09:3a:24:e4:36:d9:e9:2c:da:38:d0:73:75:61:d7:c1:6c:26:
        8b:9b:e0:d5:dc:67:ed:8c:6b:33:d7:74:22:3c:4c:db:b5:8d:
        2a:ce:2c:0d:08:59:05:09:05:a6:39:9f:b3:67:1b:e2:83:e5:
        e1:8f:53:f6:67:93:c7:f9:6f:76:44:58:12:e8:3a:d4:97:e7:
        e9:c0:3e:a8:7a:72:3d:87:53:1f:e5:2c:84:84:e7:9a:9e:7f:
        66:d9:1f:9b:f5:13:48:b0:4d:14:d1:de:b2:24:d9:78:7d:f5:
        35:cc:58:19:d1:d2:99:ef:4d:73:f8:1f:89:d4:5a:d0:52:ce:
        09:f5:b1:46:51:6a:00:8e:3b:cc:6f:63:01:00:99:ed:9d:a6:
        08:60:cd:32:18:d0:73:e0:58:71:d9:e5:d2:53:d7:8d:d0:ca:
        e9:5d:2a:0a:0d:5d:55:ec:21:50:17:16:e6:06:4a:cd:5e:de:
        f7:e0:e9:54
-----BEGIN CERTIFICATE-----
MIIDhzCCAm+gAwIBAgIBADANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTEwMjEyMTQ0NDAwWhcNMjEwMjEyMTQ0NDAwWjA7MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDA3zf8F7vglp0/ht6WMn1EpRagzSHx
```

mdTs6st8GFgIlKXsm8WL3xoemTiZhx57wI053zhdcHgH057Zk+i5clHFzqMwUqny
50BwFMtEonILwuVA+T7lpg6z+exKY8C4KQB0nFc7qKUEkHHxvYPZP9al4jwqj+8n
YMPGn8u67GB9t+aEMr5P+1gmIgNb1LTV+/Xjli5wwOQuvfwu7uJBVcA0Ln0kcmnL
R7EUQIN9Z/SG9jGr8XmksrUuEvmEF/Bibyc+E1ixVA0hmnM3oTDPb5Lc9un8rNsu
KNF+AksjoBXyOGVkCeoMbo4bF6BxyLObyavpw/LPh5aPgAIynplYb6LVAgMBAAGj
gZUwgZIwDAYDVR0TBAUwAwEB/zAdBgNVHQ4EFgQUtFrkpbPe0lL2udWmlQ/rPrzH
/f8wYwYDVR0jBFwwWoAUtFrkpbPe0lL2udWmlQ/rPrzH/f+hP6Q9MDsxCzAJBgNV
BAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEZMBcGA1UEAxMQUG9sYXJTU0wgVGVz
dCBDQYIBADANBgkqhkiG9w0BAQUFAAOCAQEAuP1U2ABUkIslsCfdlc2i94QHHYeJ
SsR4EdgHtdciUI5I62J6Mom+Y0dT/7a+8S6MVMCZP6C5NyNyXw1GWY/YR82XTJ8H
DBJiCTok5DbZ6SzaONBzdWHXwWwmi5vg1dxn7YxrM9d0IjxM27WNKs4sDQhZBQkF
pjmfs2cb4oPl4Y9T9meTx/lvdkRYEug61Jfn6cA+qHpyPYdTH+UshITnmp5/Ztkf
m/UTSLBNFNHesiTZeH31NcxYGdHSme9Nc/gfidRa0FLOCfWxRlFqAI47zG9jAQCZ
7Z2mCGDNMhjQc+BYcdnl0lPXjdDK6V0qCg1dVewhUBcW5gZKzV7e9+DpVA==
-----END
CERTIFICATE-----
-----BEGIN EC PRIVATE KEY-----
MIHaAgEBBEA3LJd49p9ybLyj9KJo8WtNYX0QKA15pqApzVGHn+EBKTTf5TlUVTN9
9pBtx9bS7qTbsgZcAij3Oz7XFkgOfXHSoAsGCSskAwMCCAEBDaGBhQOBggAEOLfs
krYcXGx/vCik7HWdSPzU4uN03v1cSWilTb73UQ5ReIb7/DjqOapSk1nXCnFWw108
usfOd2vbJR3WS85xI0Qk7nBJ7tBy8NvE15mW4XXVV+JjdjrpcJXAgec+fbLjitw9
TJoEh7Ht6HbcH8phyQLpodhyK4YSko8YokhFWRo=
-----END EC PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDkwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTAwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAR6jlGKbJd5
hiDxN789gkOcwpyHI9wRwCrADAOwOkMePBPRlwGdm7mw7Z/EAmu26zRm/hcyrs4M
qk2LabDjPI9Xo4GJMIGGMB0GA1UdDgQWBBQtxZSLJAkEz+2RKMQexM6EtsfgcjBX
BgNVHSMEUDBOgBT6gyXHzPIPYc1Vr1aGiLLeMh4HpqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA4ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgP7S8vFstfUBdNe6ym5GYG5Q+aBVEKqRs
fVW7HNUktSYCIQDo6Jua6o/DJbrpq4qYWq5gv4yGyzPTN+3IaKrEICdaaw==
-----END CERTIFICATE-----
DES check weak key #1
des_check_weak:"0101010101010101":1

DES check weak key #2
des_check_weak:"FEE0FEE0FEF1FEF1":1

DES check weak key #3
des_check_weak:"0101010101010100":0

DES check weak key #4
des_check_weak:"EEE0FEE0FEF1FEF1":0

DES Encrypt OpenSSL Test Vector #1

des_encrypt_ecb:"0000000000000000":"0000000000000000":"8CA64DE9C1B123A7"

DES Encrypt OpenSSL Test Vector #2
des_encrypt_ecb:"FFFFFFFFFFFFFFFF":"FFFFFFFFFFFFFFFF":"7359B2163E4EDC58"

DES Encrypt OpenSSL Test Vector #3
des_encrypt_ecb:"3000000000000000":"1000000000000001":"958E6E627A05557B"

DES Encrypt OpenSSL Test Vector #4
des_encrypt_ecb:"1111111111111111":"1111111111111111":"F40379AB9E0EC533"

DES Encrypt OpenSSL Test Vector #5
des_encrypt_ecb:"0123456789ABCDEF":"1111111111111111":"17668DFC7292532D"

DES Encrypt OpenSSL Test Vector #6
des_encrypt_ecb:"1111111111111111":"0123456789ABCDEF":"8A5AE1F81AB8F2DD"

DES Encrypt OpenSSL Test Vector #7
des_encrypt_ecb:"0000000000000000":"0000000000000000":"8CA64DE9C1B123A7"

DES
Encrypt OpenSSL Test Vector #8
des_encrypt_ecb:"FEDCBA9876543210":"0123456789ABCDEF":"ED39D950FA74BCC4"

DES Encrypt OpenSSL Test Vector #9
des_encrypt_ecb:"7CA110454A1A6E57":"01A1D6D039776742":"690F5B0D9A26939B"

DES Encrypt OpenSSL Test Vector #10
des_encrypt_ecb:"0131D9619DC1376E":"5CD54CA83DEF57DA":"7A389D10354BD271"

DES Encrypt OpenSSL Test Vector #11
des_encrypt_ecb:"07A1133E4A0B2686":"0248D43806F67172":"868EBB51CAB4599A"

DES Encrypt OpenSSL Test Vector #12
des_encrypt_ecb:"3849674C2602319E":"51454B582DDF440A":"7178876E01F19B2A"

DES Encrypt OpenSSL Test Vector #13
des_encrypt_ecb:"04B915BA43FEB5B6":"42FD443059577FA2":"AF37FB421F8C4095"

DES Encrypt OpenSSL Test Vector #14
des_encrypt_ecb:"0113B970FD34F2CE":"059B5E0851CF143A":"86A560F10EC6D85B"

DES Encrypt OpenSSL Test Vector #15
des_encrypt_ecb:"0170F175468FB5E6":"0756D8E0774761D2":"0CD3DA020021DC09"

DES Encrypt OpenSSL Test Vector #16
des_encrypt_ecb:"43297FAD38E373FE":"762514B829BF486A":"EA676B2CB7DB2B7A"

DES Encrypt OpenSSL
Test Vector #17
des_encrypt_ecb:"07A7137045DA2A16":"3BDD119049372802":"DFD64A815CAF1A0F"

DES Encrypt OpenSSL Test Vector #18
des_encrypt_ecb:"04689104C2FD3B2F":"26955F6835AF609A":"5C513C9C4886C088"

DES Encrypt OpenSSL Test Vector #19
des_encrypt_ecb:"37D06BB516CB7546":"164D5E404F275232":"0A2AEEAE3FF4AB77"

DES Encrypt OpenSSL Test Vector #20
des_encrypt_ecb:"1F08260D1AC2465E":"6B056E18759F5CCA":"EF1BF03E5DFA575A"

DES Encrypt OpenSSL Test Vector #21
des_encrypt_ecb:"584023641ABA6176":"004BD6EF09176062":"88BF0DB6D70DEE56"

DES Encrypt OpenSSL Test Vector #22
des_encrypt_ecb:"025816164629B007":"480D39006EE762F2":"A1F9915541020B56"

DES Encrypt OpenSSL Test Vector #23
des_encrypt_ecb:"49793EBC79B3258F":"437540C8698F3CFA":"6FBF1CAFCFFD0556"

DES Encrypt OpenSSL Test Vector #24
des_encrypt_ecb:"4FB05E1515AB73A7":"072D43A077075292":"2F22E49BAB7CA1AC"

DES Encrypt OpenSSL Test Vector #25
des_encrypt_ecb:"49E95D6D4CA229BF":"02FE55778117F12A":"5A6B612CC26CCE4A"

DES Encrypt OpenSSL Test
Vector #26
des_encrypt_ecb:"018310DC409B26D6":"1D9D5C5018F728C2":"5F4C038ED12B2E41"

DES Encrypt OpenSSL Test Vector #27
des_encrypt_ecb:"1C587F1C13924FEF":"305532286D6F295A":"63FAC0D034D9F793"

DES Encrypt OpenSSL Test Vector #28
des_encrypt_ecb:"0101010101010101":"0123456789ABCDEF":"617B3A0CE8F07100"

DES Encrypt OpenSSL Test Vector #29
des_encrypt_ecb:"1F1F1F1F0E0E0E0E":"0123456789ABCDEF":"DB958605F8C8C606"

DES Encrypt OpenSSL Test Vector #30
des_encrypt_ecb:"E0FEE0FEF1FEF1FE":"0123456789ABCDEF":"EDBFD1C66C29CCC7"

DES Encrypt OpenSSL Test Vector #31
des_encrypt_ecb:"0000000000000000":"FFFFFFFFFFFFFFFF":"355550B2150E2451"

DES Encrypt OpenSSL Test Vector #32

des_encrypt_ecb:"FFFFFFFFFFFFFFFF":"0000000000000000":"CAAAAF4DEAF1DBAE"

DES Encrypt OpenSSL Test Vector #33
des_encrypt_ecb:"0123456789ABCDEF":"0000000000000000":"D5D44FF720683D0D"

DES Encrypt OpenSSL Test Vector #34
des_encrypt_ecb:"FEDCBA9876543210":"FFFFFFFFFFFFFFFF":"2A2BB008DF97C2F2"

DES Decrypt OpenSSL Test Vector #1
des_decrypt_ecb:"0000000000000000":"8CA64DE9C1B123A7":"0000000000000000"

DES
Decrypt OpenSSL Test Vector #2
des_decrypt_ecb:"FFFFFFFFFFFFFFFF":"7359B2163E4EDC58":"FFFFFFFFFFFFFFFF"

DES Decrypt OpenSSL Test Vector #3
des_decrypt_ecb:"3000000000000000":"958E6E627A05557B":"1000000000000001"

DES Decrypt OpenSSL Test Vector #4
des_decrypt_ecb:"1111111111111111":"F40379AB9E0EC533":"1111111111111111"

DES Decrypt OpenSSL Test Vector #5
des_decrypt_ecb:"0123456789ABCDEF":"17668DFC7292532D":"1111111111111111"

DES Decrypt OpenSSL Test Vector #6
des_decrypt_ecb:"1111111111111111":"8A5AE1F81AB8F2DD":"0123456789ABCDEF"

DES Decrypt OpenSSL Test Vector #7
des_decrypt_ecb:"0000000000000000":"8CA64DE9C1B123A7":"0000000000000000"

DES Decrypt OpenSSL Test Vector #8
des_decrypt_ecb:"FEDCBA9876543210":"ED39D950FA74BCC4":"0123456789ABCDEF"

DES Decrypt OpenSSL Test Vector #9
des_decrypt_ecb:"7CA110454A1A6E57":"690F5B0D9A26939B":"01A1D6D039776742"

DES Decrypt OpenSSL Test Vector #10
des_decrypt_ecb:"0131D9619DC1376E":"7A389D10354BD271":"5CD54CA83DEF57DA"

DES
Decrypt OpenSSL Test Vector #11
des_decrypt_ecb:"07A1133E4A0B2686":"868EBB51CAB4599A":"0248D43806F67172"

DES Decrypt OpenSSL Test Vector #12
des_decrypt_ecb:"3849674C2602319E":"7178876E01F19B2A":"51454B582DDF440A"

DES Decrypt OpenSSL Test Vector #13
des_decrypt_ecb:"04B915BA43FEB5B6":"AF37FB421F8C4095":"42FD443059577FA2"

DES Decrypt OpenSSL Test Vector #14
des_decrypt_ecb:"0113B970FD34F2CE":"86A560F10EC6D85B":"059B5E0851CF143A"

DES Decrypt OpenSSL Test Vector #15
des_decrypt_ecb:"0170F175468FB5E6":"0CD3DA020021DC09":"0756D8E0774761D2"

DES Decrypt OpenSSL Test Vector #16
des_decrypt_ecb:"43297FAD38E373FE":"EA676B2CB7DB2B7A":"762514B829BF486A"

DES Decrypt OpenSSL Test Vector #17
des_decrypt_ecb:"07A7137045DA2A16":"DFD64A815CAF1A0F":"3BDD119049372802"

DES Decrypt OpenSSL Test Vector #18
des_decrypt_ecb:"04689104C2FD3B2F":"5C513C9C4886C088":"26955F6835AF609A"

DES Decrypt OpenSSL Test Vector #19
des_decrypt_ecb:"37D06BB516CB7546":"0A2AEEAE3FF4AB77":"164D5E404F275232"

DES
Decrypt OpenSSL Test Vector #20
des_decrypt_ecb:"1F08260D1AC2465E":"EF1BF03E5DFA575A":"6B056E18759F5CCA"

DES Decrypt OpenSSL Test Vector #21
des_decrypt_ecb:"584023641ABA6176":"88BF0DB6D70DEE56":"004BD6EF09176062"

DES Decrypt OpenSSL Test Vector #22
des_decrypt_ecb:"025816164629B007":"A1F9915541020B56":"480D39006EE762F2"

DES Decrypt OpenSSL Test Vector #23
des_decrypt_ecb:"49793EBC79B3258F":"6FBF1CAFCFFD0556":"437540C8698F3CFA"

DES Decrypt OpenSSL Test Vector #24
des_decrypt_ecb:"4FB05E1515AB73A7":"2F22E49BAB7CA1AC":"072D43A077075292"

DES Decrypt OpenSSL Test Vector #25
des_decrypt_ecb:"49E95D6D4CA229BF":"5A6B612CC26CCE4A":"02FE55778117F12A"

DES Decrypt OpenSSL Test Vector #26
des_decrypt_ecb:"018310DC409B26D6":"5F4C038ED12B2E41":"1D9D5C5018F728C2"

DES Decrypt OpenSSL Test Vector #27
des_decrypt_ecb:"1C587F1C13924FEF":"63FAC0D034D9F793":"305532286D6F295A"

DES Decrypt OpenSSL Test Vector #28
des_decrypt_ecb:"0101010101010101":"617B3A0CE8F07100":"0123456789ABCDEF"

DES

Decrypt OpenSSL Test Vector #29
des_decrypt_ecb:"1F1F1F1F0E0E0E0E":"DB958605F8C8C606":"0123456789ABCDEF"

DES Decrypt OpenSSL Test Vector #30
des_decrypt_ecb:"E0FEE0FEF1FEF1FE":"EDBFD1C66C29CCC7":"0123456789ABCDEF"

DES Decrypt OpenSSL Test Vector #31
des_decrypt_ecb:"0000000000000000":"355550B2150E2451":"FFFFFFFFFFFFFFFF"

DES Decrypt OpenSSL Test Vector #32
des_decrypt_ecb:"FFFFFFFFFFFFFFFF":"CAAAAF4DEAF1DBAE":"0000000000000000"

DES Decrypt OpenSSL Test Vector #33
des_decrypt_ecb:"0123456789ABCDEF":"D5D44FF720683D0D":"0000000000000000"

DES Decrypt OpenSSL Test Vector #34
des_decrypt_ecb:"FEDCBA9876543210":"2A2BB008DF97C2F2":"FFFFFFFFFFFFFFFF"

DES-CBC Encrypt OpenSSL Test Vector #1
des_encrypt_cbc:"0123456789abcdef":"fedcba9876543210":"37363534333231204E6F7720697320746865207469
6D6520":"ccd173ffab2039f4acd8aefddfd8a1eb468e91157888ba68":0

DES-CBC Decrypt OpenSSL Test Vector #1
des_decrypt_cbc:"0123456789abcdef":"fedcba9876543210":"ccd173ffab2039f4acd8aefddfd8a1eb468e91157888ba
68":"37363534333231204E6F7720697320746865207469 6D6520":0

3DES-ECB
2Key Encrypt OpenSSL Test Vector #1
des3_encrypt_ecb:2:"0000000000000000FFFFFFFFFFFFFFFF":"0000000000000000":"9295B59BB384736E"

3DES-ECB 2Key Encrypt OpenSSL Test Vector #2
des3_encrypt_ecb:2:"FFFFFFFFFFFFFFFF3000000000000000":"FFFFFFFFFFFFFFFF":"199E9D6DF39AA816"

3DES-ECB 2Key Decrypt OpenSSL Test Vector #1
des3_decrypt_ecb:2:"0000000000000000FFFFFFFFFFFFFFFF":"9295B59BB384736E":"0000000000000000"

3DES-ECB 2Key Decrypt OpenSSL Test Vector #2
des3_decrypt_ecb:2:"FFFFFFFFFFFFFFFF3000000000000000":"199E9D6DF39AA816":"FFFFFFFFFFFFFFFF"

3DES-CBC 3Key Encrypt OpenSSL Test Vector #1
des3_encrypt_cbc:3:"0123456789abcdeff1e0d3c2b5a49786fedcba9876543210":"fedcba9876543210":"3736353433
3231204E6F7720697320746865207469 6D6520":"3FE301C962AC01D02213763C1CBD4CDC799657C064ECF5
D4":0

3DES-CBC 3Key Decrypt OpenSSL Test Vector #1
des3_decrypt_cbc:3:"0123456789abcdeff1e0d3c2b5a49786fedcba9876543210":"fedcba9876543210":"3FE301C96
2AC01D02213763C1CBD4CDC799657C064ECF5D4":"37363534333231204E6F7720697320746865207469 6D65
20":0

DES-CBC
Encrypt (Invalid input length)
des_encrypt_cbc:"0123456789abcdef":"fedcba9876543210":"37363534333231204E6F7720697320746865207469
D65":"":MBEDTLS_ERR_DES_INVALID_INPUT_LENGTH

3DES-CBC 3Key Encrypt (Invalid input length)
des3_encrypt_cbc:3:"0123456789abcdeff1e0d3c2b5a49786fedcba9876543210":"fedcba9876543210":"3736353433
3231204E6F7720697320746865207469D65":"":MBEDTLS_ERR_DES_INVALID_INPUT_LENGTH

Run through parity bit tests
des_key_parity_run:

DES Selftest
des_selftest:
SSL DTLS replay: initial state, seqnum 0
ssl_dtls_replay:"":"000000000000":0

SSL DTLS replay: 0 seen, 1 arriving
ssl_dtls_replay:"000000000000":"000000000001":0

SSL DTLS replay: 0 seen, 0 replayed
ssl_dtls_replay:"000000000000":"000000000000":-1

SSL DTLS replay: 0-1 seen, 2 arriving
ssl_dtls_replay:"000000000000,000000000001":"000000000002":0

SSL DTLS replay: 0-1 seen, 1 replayed
ssl_dtls_replay:"000000000000,000000000001":"000000000001":-1

SSL DTLS replay: 0-1 seen, 0 replayed
ssl_dtls_replay:"000000000000,000000000001":"000000000000":-1

SSL DTLS replay: new
ssl_dtls_replay:"abcd12340000,abcd12340001,abcd12340003":"abcd12340004":0

SSL DTLS replay: way new
ssl_dtls_replay:"abcd12340000,abcd12340001,abcd12340003":"abcd12350000":0

SSL DTLS replay: delayed
ssl_dtls_replay:"abcd12340000,abcd12340001,abcd12340003":"abcd12340002":0

SSL DTLS replay: lastest replayed
ssl_dtls_replay:"abcd12340000,abcd12340001,abcd12340003":"abcd12340003":-1

SSL DTLS replay: older replayed
ssl_dtls_replay:"abcd12340000,abcd12340001,abcd12340003":"abcd12340001":-1

SSL
DTLS replay: most recent in window, replayed
ssl_dtls_replay:"abcd12340000,abcd12340002,abcd12340003":"abcd12340002":-1

SSL DTLS replay: oldest in window, replayed
ssl_dtls_replay:"abcd12340000,abcd12340001,abcd1234003f":"abcd12340000":-1

SSL DTLS replay: oldest in window, not replayed
ssl_dtls_replay:"abcd12340001,abcd12340002,abcd1234003f":"abcd12340000":0

SSL DTLS replay: just out of the window
ssl_dtls_replay:"abcd12340001,abcd12340002,abcd1234003f":"abcd1233ffff":-1

SSL DTLS replay: way out of the window
ssl_dtls_replay:"abcd12340001,abcd12340002,abcd1234003f":"abcd12330000":-1

SSL DTLS replay: big jump then replay
ssl_dtls_replay:"abcd12340000,abcd12340100":"abcd12340100":-1

SSL DTLS replay: big jump then new
ssl_dtls_replay:"abcd12340000,abcd12340100":"abcd12340101":0

SSL DTLS replay: big jump then just delayed
ssl_dtls_replay:"abcd12340000,abcd12340100":"abcd123400ff":0

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price.

Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for

this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid
anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate to certain responsibilities for you if you
distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether
gratis or for a fee, you must give the recipients all the rights that
you have. You must make sure that they, too, receive or can get the
source code. And you must show them these terms so they know their
rights.

We protect your rights with two steps: (1) copyright the software, and
(2) offer you this license which
gives you legal permission to copy,
distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain
that everyone understands that there is no warranty for this free
software. If the software is modified by someone else and passed on, we
want its recipients to know that what they have is not the original, so
that any problems introduced by others will not reflect on the original
authors' reputations.

Finally, any free program is threatened constantly by software
patents. We wish to avoid the danger that redistributors of a free
program will individually obtain patent licenses, in effect making the
program proprietary. To prevent this, we have made it clear that any
patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and
modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains
a notice placed by the copyright holder saying it may be distributed
under the terms of this General Public License. The "Program", below,
refers to any such program or work, and a "work based on the Program"
means either the Program or any derivative work under copyright law:
that is to say, a work containing the Program or a portion of it,
either verbatim or with modifications and/or translated into another
language. (Hereinafter, translation is included without limitation in
the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work

are not derived from the Program,
and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution
and only if you
received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary

form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source
code, even though third parties are not
compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing
or modifying
the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For
example, if a patent
license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then

the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free

Software Foundation, write to the Free Software Foundation; we sometimes
make exceptions for this. Our decision will be guided by the two goals
of preserving the free status of all derivatives of our free software and
of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE,
THERE IS NO WARRANTY
FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR
THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest
possible use to the public, the best way to achieve this is to make it
free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest
to attach them to the start of each source file to most effectively
convey the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU

General Public License as published by
the Free Software Foundation; either version 2 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License along
with this program; if not, write to the Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute
it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this
is what you want to do, use the GNU Lesser General
Public License instead of this License.
-----BEGIN PUBLIC KEY-----
MHYwEAYHKoZIzj0CAQYFK4EEACIDYgAE2cZitQuinKR5kEUOBDrq9PDGmxVnbREv
YipxyTBZr5mWkcVoDStE0RFXnbEvSkE6LtXEX8+2e1tj4AuR6+WdCaaxrCwMQoKq

EjF+1ZFPmZvEiLsTLoNCzDbyyl4zecdH
-----END PUBLIC KEY-----
-----BEGIN X509 CRL-----
MIIBcTCB9wIBATAKBggqhkjOPQQDAjA+MQswCQYDVQQGEwJOTDERMA8GA1UEChMI
UG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EXDTEzMDkyNDE2
MzEwOFoXDTIzMDkyMjE2MzEwOFowFDASAgEKFw0xMzA5MjQxNjI4MzhaoHIwcDBu
BgNVHSMEZzBlgBSdbSAkSQE/K8t4tRm8fiTJ2/s2fKFCpEAwPjELMAkGA1UEBhMC
TkwxETAPBgNVBAoTCFBvbGFyU1NMMRwwGgYDVQQDExNQb2xhcnNzbCBUZXN0IEVD
IENBggkAwUPifmJDzOgwCgYIKoZIzj0EAwIDaQAwZgIxAKuQ684s7gyhtxKJr6Ln
S2BQ02f1jjPHrZVdXaZvm3C5tGi2cKkoK1aMiyC3LsRCuAIxAIMhj0TmcuIZr5fX
g5RByD7zUnZBpoEAdgxFy4JPJ2IViWOPekSGh8b/JY1VNS6Zbw==
-----END X509 CRL-----
-----BEGIN X509 CRL-----
MIIBqzCBlDANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDERMA8GA1UEChMI
UG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EXDTExMDIyMDEwMjI1
OVoXDTE5MTEyNTEwMjI1OVowKDASAgEBFw0xMTAyMTIxNDQ0MDdaMBICAQMXDTEx
MDIxMjE0NDQwN1owDQYJKoZIhvcNAQEFBQADggEBAJYuWdKPdblMVWCnxpMnchuL
dqWzK2BA0RelCaGjpxuwX3NmLDm+5hKja/DJxaRqTOf4RSC3kcX8CdIldsLO96dz
//wAQdFPDhy6AFT5vKTO8ItPHDb7qFOqFqpeJi5XN1yoZGTB1ei0mgD3xBaKbp6U
yCOZJSIFomt7piT4GcgWVHLUmpyHDDeodNhYPrN0jf2mr+ECd9fQJYdz1qm0Xx+Q
NbKXDiPRmPX0qVleCZSeSp1JAmU4GoCO+96qQUpjgll+6xWya3UNj61f9sh0Zzr7
5ug2LZo5uBM/LpNR1K3TLxNCcg7uUPTn9r143d7ivJhPl3tEJn4PXjv6mlLoOgU=
-----END
 X509 CRL-----
AES-GCM NIST Validation (AES-128,128,0,0,128) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"1014f74310d1718d1cc8f65f033aaf83":"":"6bb54c9fd83c12f5ba76cc83f7650d2c":"":"":128:"0b6b57db309eff920c8133b8691e0cac":0

AES-GCM NIST Validation (AES-128,128,0,0,128) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"d874a25f2269e352ccdd83cc2d4e45b7":"":"9717abb9ed114f2760a067279c3821e3":"":"":128:"0e09e53e5fe8d818c5397c51173eda97":0

AES-GCM NIST Validation (AES-128,128,0,0,128) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"7dab77e23b901c926454f29677eb62d4":"":"8aaec11c4a0f053d7f40badd31a63e27":"":"":128:"cec2e3230d8b762acee527e184e4c0db":0

AES-GCM NIST Validation (AES-128,128,0,0,120) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"2397f163a0cb50b0e8c85f909b96adc1":"":"97a631f5f6fc928ffce32ee2c92f5e50":"":"":120:"3b74cca7bcdc07c8f8d4818de714f2":0

AES-GCM NIST Validation (AES-128,128,0,0,120) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"a7adc0d3aacef42397bbca79dd65dbdf":"":"c6d3114c1429e37314683081d484c87c":"":"":120:"d88141d27fe1748919845cfa5934bc":0

AES-GCM
NIST Validation (AES-128,128,0,0,120) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"10171805d7f7a6d87b64bda57474d7fc":"":"fad65b50c1007c4b0c83c7a6720cacb8":"":"":120:"c3d3f240d3f3da317eae42a238bcc1":0

AES-GCM NIST Validation (AES-128,128,0,0,112) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"8aaa0c85d214c6c9e9e260e62f695827":"":"84e25c916f38dd6fdb732c0d6d8f86bb":"":"":112:"a774815a2a8432ca891ef4003125":0

AES-GCM NIST Validation (AES-128,128,0,0,112) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"def8b6a58b8e582e57700bab4f2a4109":"":"3615439e9fb777439eb814256c894fb2":"":"":112:"537be9c88d3a46845e6cf5f91e11":0

AES-GCM NIST Validation (AES-128,128,0,0,112) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"5894231d743f79638687c070b60beee1":"":"e34cd13b897d1c9b8011a0e63950c099":"":"":112:"d582c4bc083a8cf1af4d5c2c9b11":0

AES-GCM
NIST Validation (AES-128,128,0,0,104) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"6b25f9cbdc3bcd27fd245a1c411594bc":"":"a6526f8c803b69dd5f59feca1cff78e2":"":"":104:"c7e19e08a09a9c1fa698202890":0

AES-GCM NIST Validation (AES-128,128,0,0,104) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"b3235422897b6459798a97ddd709db3d":"":"96679e9362f919217d5e64068969d958":"":"":104:"44ed41bda0eb0958d407b7b787":0

AES-GCM NIST Validation (AES-128,128,0,0,104) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"f65bc795434efba3c5399ed3c99ff045":"":"2e727c19a89cba6f9c04d990245fceed":"":"":104:"64830ed7f772e898800fc9ae2a":0

AES-GCM NIST Validation (AES-128,128,0,0,96) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"c6c66d50f2f76c4e911b3b17fcdcba1d":"":"77b42158a4ef5dc33039d33631bb0161":"":"":96:"1bce3ba33f73e750ab284d78":0

AES-GCM
NIST Validation (AES-128,128,0,0,96) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"13558db9b7441c585d381ffc16b32517":"":"addf5dbe0975c5ad321e14dd4bdc2ad2":"":"":96:"f413c3bf125ce5317cd1c6bd":0

AES-GCM NIST Validation (AES-128,128,0,0,96) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"74638628b1361c2954ce0ac5456a1155":"":"c5861507c879e6864d7cb1f77cc55cc6":"":"":96:"8a514fdc7835711e4f458199":0

AES-GCM NIST Validation (AES-128,128,0,0,64) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"7815d22c5c081df9ac2114aaa2c0cbf9":"":"822f83cd9f249dfc204b5957f0b0deab":"":"":64:"aa1f69f5d3bb79e5":0

AES-GCM NIST Validation (AES-128,128,0,0,64) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"1a847a47823cb9c298e4107c6aaff95c":"":"39348f80c6bc489f9315be7a6fcbb96f":"":"":64:"c3b3f31e56cf4895":0

AES-GCM NIST Validation (AES-128,128,0,0,64) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"16e67ea248ea6db08af1d810cb10574e":"":"50386e2075eb15ca3f3e6db6bff01969":"":"":64:"3d4f3b8526a376ae":0

AES-GCM
NIST Validation (AES-128,128,0,0,32) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"26a8301636ba93e7f56309143f184241":"":"c7e32b1d312971bdc344aefaf45461bc":"":"":32:"25f1b41c":0

AES-GCM NIST Validation (AES-128,128,0,0,32) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"130a07c467067148da2790f90d73ff32":"":"800b81c9d2ff3a8e15690ffb4117e211":"":"":32:"abcc8d71":0

AES-GCM NIST Validation (AES-128,128,0,0,32) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"ccfaae59c3196b8c403716424ea601f5":"":"f9b059de0efa4e3f364763d63d098410":"":"":32:"8933444f":0

AES-GCM NIST Validation (AES-128,128,0,1024,128) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"b5beefbdd23360f2dd1e6e3c1ddbfebf":"":"81a8494f85be635d71e5663789162494":"f9ebf242b616a42e2057ede3b56b4c27349fed148817a710654de75d1cfc5f6304709b46ef1e2ccb42f877c50f484f8a8c6b0a25cff61d9537c3fd0c69bbc6ef21cbec8986cbc9b6e87963b8d9db91b7134afe69d3d9dec3a76b6c645f9c5528968f27396cc9e989d589369c90bbfefb249e3fa416451bc3d6592cc5feefbd76":"":128:"159a642185e0756d46f1db57af975fa3":0

AES-GCM
NIST Validation (AES-128,128,0,1024,128) #1
depends_on:MBEDTLS_AES_C

gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"c465aa8fe5d534c912e654f5aaed5857":"":"5c155f7194b0d0a17b9a0c234d609443":"a3f8d705b233b574399f72350b256cb4893e130688913ce3def8e44687688c0352ff987aea35dc53bc95cdb9cdcc6e6eb280265d9a1af38d526392ab63c9b043c1b1b43e18321e84eb7e08884f2463c32b55eb5859fb10918595a724a61cfdf935e4f96d0721612720d46a946487b525779f6ce0abf04fc5608351119b7427d2":"":128:"9595a6d879cd7a949fa08e95d2b76c69":0

AES-GCM NIST Validation (AES-128,128,0,1024,128) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"744b9e1692d8974d7dec349ebd7fe1e8":"":"62ad4b09fd554e0d6b3937839e693e5b":"6f9978f7078f0030c45caf49128ff72943a208a2398d08d132239f3ab5c184708e4222ec9ccde69dc86d1700c2fe0af939454bbb3962327158557860b6fa492ab8201df262a6209705c7e3129419bce8b827320893c1579ca05b32c81b3963b849428f71fe7528e710557a272117199163a35ebfbaba78f7676f7e566b16311a":"":128:"634f6fe9625be8b1af9f46bcc0fa3162":0

AES-GCM
NIST Validation (AES-128,128,0,1024,120) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"097c059535037c6b358dbb5a68b5f2b1":"":"00caedfa078c27e3d9551e3fb8d98d77":"6c4bde11129a959fcd6a482cb19f5f1c582c042b314f7997b0450242f9e669dc1cbb0a3b7a185bf8b035267e6f03206268008e2b97864d44d6a9c6b1b4b067d623c4b4e9c608042ea9120aed3bee80886352683891496d8980e40b8480c98c2fe08f945aa1ef6007c65220319dd8678184ab54e81083b746ec6441e87a568e0c":"":120:"5075ef45c6326726264703f72badde":0

AES-GCM NIST Validation (AES-128,128,0,1024,120) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"d25db5eca46c16490294423ca0c35660":"":"6f37f15d6c7ea816278ab977c29fa45e":"bd76fd431cea72a288e5d7289c651c93b5f429a54f85249021d6b595eb9ce26e18914a381a6b0299acc3725431b352670f206b731be718a598ec123dce0a2c5ac0aa4641b092e704da9f967b909ca55c2722298365a50dcb5b5ec03a1d0cbb67b8de1e8b06e724af91137e0d98e7dc1e8253887da453cdcbd2eca03deacaabb8":"":120:"00510851e9682213d4124d5517ebaf":0

AES-GCM
NIST Validation (AES-128,128,0,1024,120) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"b3c6258a726aff94a7bcc41646c68157":"":"7f5b3315afe5167a7e9061ab8b005588":"0ef3384862c7e00c2912e7fde91345dc3134b5448e6838f41135ba9199c03a7f208887e467563b39a6c1316540c1401e8ff148386c50fcf15724a65d3210b17832d63cdce76bd2b458348332b0b542122a57e381475a59440f280db6e1f4b8d0babfd47e3db11a9ef89cba5f334f0e8e72be30afb2b1ef2df8eb7f8d3da033c4":"":120:"180489039ccf4a86c5f6349fc2235b":0

AES-GCM NIST Validation (AES-128,128,0,1024,112) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"73cd0a1e2b6e12fbaa7cbace77d5119c":"":"d897681764bcc3b62c26b4aaf407cefa":"8c773e14a906c7deae362d1bf3d7e54c6be4c74c691b7f2d248693b2619219fba6eb5bc45f77af1cf7c05d3dd463158f884fe82290d145135889fd851b86ee282aa20bbdf6af78c7f9db6128b8b99e7f9b270fd222efa18f7aca6932a1024efb72113e812b3f9d2d4ccc7c85f5898ddacccbf1b441cd74097740dd922b57bade":"":112:"d8811a8990191f1e5bd15be84995":0

AES-GCM
NIST Validation (AES-128,128,0,1024,112) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"c1dfddafe076d0ceebb0f37bb25bc0b1":"":"29c56db10cea802c19fb6230227ab2bf":"287b73cdc62ce058cdceff8e9af7afc321716f69da9eef60c2de93630ba7d0ed0a9d303cd15521a2647159b8478593f3dd3f5b7c52081e5154e55ccbff371d7e5dfc2d05e14d666a01ec2cc6028aacadfd78dfc73bf639fc4dfa0a0c46415902bbda2443620fa5e0ce4fccf1b8591e3a548f95755102a8438300753ea5f61b9f":"":112:"309fedad1f3b81e51d69e4162e6f":0

AES-GCM NIST Validation (AES-128,128,0,1024,112) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"2c4087ccd28ceda147d2fcfc18579b1e":"":"9cbdd67c79ab46bcbcfa96fa2c3d7e87":"35088d18dff0a9d3929ce087668aae1d364b37a97102f3f43e11950e6ec8296d0c99b00cd1c5dff53d3a38475e7da7b9ee4ce0c6388a95d3f8b036414e4b79cd02b5468cbb277f930e7c92432a609db1effe65f60f1174b58f713e199491f9e0c29ba1f2e43306775d18c1136274af61488a2f932e95eceadfe3fe4b854fe899":"":112:"b7e83207eb313b3ceb2360bc8d4f":0

AES-GCM
NIST Validation (AES-128,128,0,1024,104) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"bb66584c8b18f44c11f3bd7180b9b11d":"":"39c82aee03ce0862ff99f8812cdbdcf0":"45ec858e0a5c6d81144ba893e0002818a70e9a19002a5471993077241b3fcfb4fd984f2450803293882d1c7ecb654e611578fe7d258f9a2ca3b5f0c0f0d0ec4828bdeb9299914ff2ac4cc997cf54fa908afdb3eae9f91d67c4637e1f9eb1eae2b3f482ddd5467668bc368b96bbbfc33b9ae2658e4ca43fcf4b66ba2a079d65f1":"":104:"24332fd35a83b1dfb75969819b":0

AES-GCM NIST Validation (AES-128,128,0,1024,104) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"7b2a230c8978d4e38fa5096ddc19d6f5":"":"cd25e744a78af858e825e1fd070324ee":"628baac336862573cee158cd3935c34df3055dadc9c1695e9ea18724f6457f0d1833aab30b85a99e0793e56000de5d6d5cb2327a4cc8bec40cd198459e7b93617713e63bbd15381a066bc44a69c9ad3dfb1984f8b33a9429eda3068d3ac5fbbaaee2b952a486e58d674ffca641d9ec1d102600af11641fd5fff725204e6c34a8":"":104:"68d49d495ff092ca8e5a2c16cb":0

AES-GCM
NIST Validation (AES-128,128,0,1024,104) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"73aa576e1dfad2c993afcc088bd8d62b":"":"712e665a0a83e8ecad97e92afeb35706":"314e5fee776e9d5d2a1fb64ceb78e2c9a560a34724e30da860b5588fe63d50838cb480ff8ac61d7958b470b1bfd4c84799af6cb74c4a331b198204a251e731f7d785b966da595b745d01769623492c18b9dd8bd3c75249effd2032658c715906a71dbbed847027ea75d647f9803296a41906e0915250854597a163035a8d3f45":"":104:"a41f5c9c7de2694c75856460d4":0

AES-GCM NIST Validation (AES-128,128,0,1024,96) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"83f7631c4d4c466c9246cbc48e2dde6f":"":"f5d6c8c252cb687a931c38f58f74943c":"1f35e94a35d0f424bf690a15038126a41502593612efe6333cf94ea0565ca6acdefae8d74dae62df95e9261c6596c3397220e044c5b08cf39cccb27315d9b795da321204910274a93436bc0573fdba04ae6bb14c6ca955

cf8b9e193a12e05796d7f4b397507614dabc457f1cd3ce19e439b6e62703f2189372938b29b7a542b9":"":96:"bb85dbd858ab7b752da7e53c":0

AES-GCM
NIST Validation (AES-128,128,0,1024,96) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"784e023b2d4c978151d05ee71533c56c":"":"f16d041b9f0f454db9985c8558ef8a61":"91f6e108c294640c7bc65d102d3d25a7bfbbe114acec9b495636689afd65fff794837946602ef04de7d4304a81809e0f7ddc45c476c29fd5286fcf4dd1ba76ed3ce88abdb51cd21e7aaeecb13238ac031da87ab96b2a13157278bf669d0efae28852ec3585d520d54502881322f7977d03954e17e7c0c0d8f762e34f59ca141e":"":96:"59699c639d67be6a6d7c9789":0

AES-GCM NIST Validation (AES-128,128,0,1024,96) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"d3a2ec66e4a72cb3540e87f4e67c7e58":"":"07a9cf9f44b07e3067d60e276322e9fb":"d7e722b82e8607a64fbfeefc7887009298f06a637fe937277e3a76e8addaeeb460ba0743912c07b500b4b51e9fec2b7eddf691d155baf689f75968160c19a8330e254220142ae843bf0687aabeb74ab607227b0a7539ec3cfea72a5c35f236623af78beffaee6e7b1adc2895732ffedb3f8520710f04eb9c2ce9b2cae215ed5c":"":96:"f29aec72368bfcfa9ae815fd":0

AES-GCM
NIST Validation (AES-128,128,0,1024,64) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"83f382a90146544ef4871bde891aed22":"":"c6f664f5ccfd1aaefb60f7fa3b642302":"656a2f221a1339d8f5c26393a08fa31859f626eec9a68afb6ee30e5b6859d1cbb5ed7dea6cbc4a5d537d70227d0608185df71a0252fa313be4d804567c162b743814f8b8306155931fdecf13822a524868b99a27fd2ff8f98c16edccd64520e2dce1ad645fd5255c7c436d9b876f592ef468397b00857ba948edf21215d63d99":"":64:"09df79dd8b476f69":0

AES-GCM NIST Validation (AES-128,128,0,1024,64) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"64334f10a62c26fef79d9024d4ba7c5f":"":"7b85251554d4f0ff89980cf3568c5caa":"dab2892262a1832a473cd3481acbd3d1820f14361c275514ec693b40f2170ea5ff82c4f7e95a7c783ea52c43a0a399c37b31319a122fd1a722e6631efa33f8bfb6dc193986580f0344d28842a3a4a5ca6880552557f3915a65501f6ee0c1b68a4c9040f0fac381cbccb6a6e9bca23b99f2ef1abbca71c69aa27af2db176bf37d":"":64:"3e8406900a4c28bc":0

AES-GCM
NIST Validation (AES-128,128,0,1024,64) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"1c98ca4971c3a6333c18b88addf13368":"":"7f617f08e826a3c61882c3e00c203d4b":"ab1531fce0f279d21091c3334bd20afa55c7155bfc275330ed45f91cfc953771cbde2582f4be279918ac8b9ae07cb3b2efd14292e094891d4841be329678ad58d714fc8ce4bffe51f539f4240c14ba883b95cdc32cf4a9fd6ba4ffeafa0d6718989c46483c96cfca3fe91000f9f923d7f96725e966de068b5da65546fe38f70e":"":64:"58cc756d3bf9b6f9":0

AES-GCM NIST Validation (AES-128,128,0,1024,32) #0
depends_on:MBEDTLS_AES_C

gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"247d3abeb807bde959e68b40a3750045":"":"3f5390cd7921fcb42c59f0db05a8a62f":"81abf375da7157a1a56068d0918037fecb7296d9b1771c54ae6030abda4b9d76feff818de81747980b2c1b005e36b3be36afbf1092edef6fd875d2903d73612addf206a6ae65886421059c70990a6ee33197f92bed649901fed62fdd20c30d81baf6090f50d9f59290528e58a0b7412ace0a293369f2b4c8d72c2fb0e1c432f5":"":32:"37bb4857":0

AES-GCM
NIST Validation (AES-128,128,0,1024,32) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"622be8cd3c757de00fbb7ab4563ce14f":"":"16c53a843b1549716d7c06b141861862":"a15d101580d549f2401bf0f36be0f83724875205c9109d2d69d2609cbf67504b918f0859303192b4075f952454f3e7152f898f997b36afc0356712fc08db3343054b20e88ad1274e019bf8fcc3c921d3bc8f9c1d1d24adc61f6033a83ef46a84762304f1903553748b13b1647c96eb8702ebb41ccea4d9cfebcb177c453277f2":"":32:"35778596":0

AES-GCM NIST Validation (AES-128,128,0,1024,32) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"8a660aa0191f9816261387d5aeb262f6":"":"c720cb31e841480da5ba656e9b93f066":"d979affe395bd048db26d26908a1c2a435905299086cc55bb65ef782f5aed99c41743c3ae252ea087f5453bdc605abd784b337b60960946358da2218b076826659a1fafa59124a00a3424fce0d00c38eea85cfb3d1e01bcb09d9870d5b3fe728f394e0e512f5aa849d0550d45a7cc384f1e4c6b2e138efbc8f586b5b5ed09212":"":32:"cf7944b1":0

AES-GCM
NIST Validation (AES-128,128,1024,0,128) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"ce0f8cfe9d64c4f4c045d11b97c2d918":"dfff250d380f363880963b42d6913c1ba11e8edf7c4ab8b76d79ccbaac628f548ee542f48728a9a2620a0d69339c8291e8d398440d740e310908cdee7c273cc91275ce7271ba12f69237998b07b789b3993aaac8dc4ec1914432a30f5172f79ea0539bd1f70b36d437e5170bc63039a5280816c05e1e41760b58e35696cebd55":"ad4c3627a494fc628316dc03faf81db8":"":"0de73d9702d9357c9e8619b7944e40732ac2f4dd3f1b42d8d7f36acb1f1497990d0ec3d626082cdb1384ec72a4c1d98955ba2a3aae6d81b24e9ce533eb5ede7210ae4a06d43f750138b8914d754d43bce416fee799cc4dd03949acedc34def7d6bde6ba41a4cf03d209689a3ad181f1b6dcf76ca25c87eb1c7459cc9f95ddc57":128:"5f6a3620e59fe8977286f502d0da7517":0

AES-GCM NIST Validation (AES-128,128,1024,0,128) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"81371acd5553fdadc6af96fdeee4c64d":"940806fd5ddcab9937b4ba875e46bb4b7e9688d616d17fd24646f1ef1457819f55887f53bd70039bb83b4d346aabe805288ab7a5756874bdc2b3d4894217d3a036da5e9e162fa2d9819ceb561ecf817efc9493b9a60796f6dc5e717ac99bc4ba298eee4f3cd56bbc07dde970d4f07bbfa1f5fe18c29a3927abe11369091df28f":"3262501ed230bc4f5a190ab050e1bcee":"":"ffeb1907bdbfea877890a6e972a533ae661a903a257b3b912c7c768cc988e05afd71a9e6117d90d1e1b54f55de9b10cbce7a109452567483cc8d6a68b9e56da10802630591fdd8d55f9e172f0f58a7e0c56a73a1ae3c3062f0997b364eb0885d48e039b2ba1bd14dbb9c74a41cbd4b52564e470d1a8038d15207a7650bd3f1d6":128:"227d422f8797b58aa6a189658b770da9":0

AES-GCM
NIST Validation (AES-128,128,1024,0,128) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"ef5295e9ae74729e222df6dab251158d":"59372848432f86f5

740500391d2e5d5fbe1f80ea876a0ecb9a5b298d9ea7cdc28620aeb2fda015345ae476f265351b2c6b6fcd66bc8aae4dc
8a95c1350cda204da3d2d2fc5e6e142dc448296d5df0cc349d1eba2fa98d2f468662616274a147fbe07927440afa3967a
c09a03a8de0b03f3036bde5e272e3c4c5ff169dd730238":"194d08fcc3c08ab96fa724c381274d3f":"":"fdceeffdc8390b
de6b910544db61db2f345eba0664f78f65d94b90e3e2a5251be374b3c5d881460cfff3549a01f84eb9d54087306a20f51
56cd555e46bd2173386c90ea47983320fcbf24e09a05f2ec4b2577287d05e050b55b3002b753de49abef895ee9701581
0c06d09212b0c09e4910c64ac3981795a1e360197740360fd":128:"e94603dbd8af99ab1e14c602a38a0328":0

AES-GCM
NIST Validation (AES-128,128,1024,0,120) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"26db035f2ddd9f5672c6f6af156838d7":"92c3159368476497
56b0b1bb4a3453e6e6da866f8088d96da44412d9f47a22dda0cd817287ba42163be59a69f73963059139fb3ba44bc5eb
fd95b6742546dfb4fe95608dca71911d1347be68179d99c9ebf7ee1d56b17195f8794f3a658d7cad2317ed1d4bc246cd4
530e17147e9ecdf41091a411a98bb6047eee8b4f1e4a9ef":"3686d49bb8c7bd15546d453fdf30e1f3":"":"1ac98e9ccfe6
3a2f12a011e514f446c4c0e22dd93613b1b9b8f56d148be8a24e3682dfc1cde2b69e72d200b516a99e7466dae8cc678c6
117dc14b2364cd2b952aed59722056d7dae4cfdb7d9c4f716aef2aa91a4f161d01c98d92d974247bb972de0557e17517
7ce34361be40c30ab9ac46240016e5ad350c3b7232c5920e051":120:"b744316880b0df3d4f90c3ffa44144":0

AES-GCM
NIST Validation (AES-128,128,1024,0,120) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"d5c63757197a132cbb33351fd2d81a46":"e970b62ce5f06b1
5f8448aa2a095c2b3c8adf535e110e7f374411ed51fa19f9c4926045f796b7cd8a942b6a19811b7aae59fce37e50d6ca5a
4a57bfb041a5b51c1ee82b54d03be22d9dc2bb9a2e708503b85e2479b0425a033ae825b4f232ca373e280e3cc97cf0d7
9397a81fb30d3b41cdaa3e788470cde86734e10a58b1e3a":"a669a4d2f841f9a0b9ede1fb61fee911":"":"522ba7220d0
d4bea7ab9ca74ad8fa96ba337f7aa749cd26186499081ba325df6d6b90a81bd1c7adda0cd1ca065894f14a074ec13eff11
7b2a00042038aea55850056a63adf04f58fcd7269085f5ad1ef17ce7b6c40804127f14747a2ad93ec31fada83663af025a
3b90c20a4ae415b1c960094e5fd57db0d93a81edcce64f72d":120:"7bfce3c8e513a89a5ee1480db9441f":0

AES-GCM NIST Validation (AES-128,128,1024,0,120) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"f380d3bf0d55a1cd56b7e78359eb6c66":"c0e977e91c1c50ee
78d4a56c527b2d31a1a14f261aa77e52d910f8f230de4908b5cc6943e28b8c6e7ac61eebe270dcfde48d140ec13792371
932e545b6ef4b52d1dfdf54c60ff892b74095a3f4a2b9000acd2cac04666a2305343b8c09f89dcc0c25bbe2a39b146241
18df025962edec3dfc58d36fcac531b291ec45b5159e22":"ba3300f3a01e07dde1708343f01304d4":"":"752f09b51861
6a91a802cf181532c7ec65b54c59c1bab3860f0ad19971a9e5bc8843524c5ffac827067b462ebb328e2eff4dd931728de
882055129997204e78717becd66e1f6c9e8a273c4251896343604ac289eb1880207a8ea012626e18e69ad7573ef73071
b8e2fb22c75c7fc7bf22382d55a5d709c15e4e8ff14e2bf81e4":120:"fbf8818aee5c71ebfd19b0bcd96a7a":0

AES-GCM
NIST Validation (AES-128,128,1024,0,112) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"47c807cd1cf181040a4e3b1d94659db8":"c4a52c1f1f0d32c2
1fb85fba21d1b358b332efa066c7893c566b2e859efdde99fc67bb6167cdb0485a8ed53dd1068d90bc990f360b0440397
91be6048ba0ee4ce1090c9fce602af59d69069f5bff8b6219aaaed5a9b1bfc8c5b7250c5a6cfe86586fa8064124d551da3
8d429a17696eb1a7a0341c363f010eafd26683eecdf82":"9963a3fb156beacd6dd88c15e83929df":"":"e784ab006de8a
52de1d04bc2c680d847c5decdd777cb2475ad4ab1dc529882d9e51cff5451b14ea5ff9a9bab5c5474e8a331d79564acdb
2ac8159e0f46e9019bf80650c481fdaf1680cadcb8c5de9f924760b376ce5736cc4970cb8715b5999f577436283a4c214

69306840af36d1e069616157d1b9ce75de3adb13d201cdf1b":112:"51e8ce23f415a39be5991a7a925b":0

AES-GCM
NIST Validation (AES-128,128,1024,0,112) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"a0b033d14fe902aa0892b0e87f966c41":"1cc751d890cd1024
86d81c618c23fa335067ac324ef11f7eddc937853db6e16d0f73727725a5a5bd580705416ecd97e368464ed0aea923ffb
71c23c37f9cf9c8bd81cdbdc3d0ac34a875db3167ec1d519004d4fa4bba041af67af1ed3d4e09c32b3e8e10abd91f4683
6cec74b1f9c5b06c05f3b18caa78e7ff185db212b52ce0":"ad4dee18e6c19433ad52021164f8afb7":"":"a30044582dacf
57332b04402e993831df0a4c1364a83c9bce7353979fb444cd1b3fe747e2c933457ff21f39e943a38a85457bfe99dc09af
886734d6e4218fc65138055ad8eb5d3044f4eed658e312b6165199e682ffa226558dc4b516f8d519f149bb5a40d2bb7d
59ece9e5fd05358c89e635792ad20c73c174719f9b28c7358":112:"6a18a4f880ce9e6796e1086ed05b":0

AES-GCM
NIST Validation (AES-128,128,1024,0,112) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"c4030ca84f132bfabaf660e036f56377":"a8fe98e2b4880d12c
99c9d5193b3537b3fbc5165cc1327395174d989be5741f867332271cdc52ddb295ddbeba33698073054c6d2416fafaeb
0a76aad870a6fb6097a29fba99f858d49418572c8e4dc0d074ca8af7727c773c8617495b1195d6b2687a2e37fad116dd7
21b60bcb5471d548c6dafe3ecdcf0c962e4659a61f4df3":"975df9c932a46d54d677af8a6c9c9cc3":"":"86b20fecebc4cf
88a6a382d693117cd2a3c9eab747bf5df5f1d35e341d204d8fea6694b92552e347da676bc8d3353984e96472a509f520
8ce100a2a9232478417947f85f10993c9d6939c8138bd6151aef8e2038536e8ba1ba84442e27586c1b642f9505455c73
8e9fd2c1b2527d1ecd3a2f6ed6e3869000ef68417ec99ff7a2":112:"3516909124c0c1f9c30453c90052":0

AES-GCM NIST Validation (AES-128,128,1024,0,104) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"6e210de363f170a7ccb1b9cec8d34737":"89853fa002985a45
651f2a7db2b45b7e7a7d33ce6c438ec4533c7fa257e1a384130369a68184a807fd0d92a70d91d7ddc56e5c5172c87225
7230d7aeb9293d785b1b8835dcde753798caff4abcd8bbc5378cd505dcf904aa69902e4f38699be972099adffc8778bd8
44a9a03e6b58a721a73324d956f20f2ffd00d3491f72f42":"39fe20b051ba21319a745349d908c4bf":"":"ac9d74f8f405
fd482287a4a7fa359caca095c0f1b46744f19c3c11e13b0c605b9857c8cc5a1754b95bcc658416f463bf8764f37320594
1885948259916eaabd964f2d6c2d784f928dc5eefe331f6c04b4862d4c8e966530de6bf533a10818de852de3af7f521b1
67cb4eb7141ba8ae8a17be1eb714fd26a474bbbbe870a659dc":104:"7a2dfc88ad34d889f5e344ee0e":0

AES-GCM
NIST Validation (AES-128,128,1024,0,104) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"6bbfeda23ea644fb37666b05dc47f590":"a85ec4c2c160deda
7e3de0ae449eea6ed1d24e2c8f3d5151f2ac0fd869f5a763981733b68f46c5197d76c26cce7ddc8afc6cdf4536d771cf3e
9cef0098e270c5e1ff72cb0ad7f84abf44b726e0eae052d0c1553afc67c7289a43851a4d04c2856cc46b4039380436465a
3b19deb56e41b859aecaf22b90578a23288d5f7d9b0e":"9d154f3cc2c5b0bdd77e86e351220960":"":"dbe575ea04b58
429e68c733d99d7fb3a57e5604d6fc3baf17e0c6f981d78c070144702861316f892023515f20b697a8f3a40d821162dc9
255d4775e7578285acf2cca67e902c060f80eaae29b9c011b6c110371409d914782e1e4115dc59439a2823507330852f
10436b121538f22a3b619075610f1da87b6035138d78c75a79":104:"8698763c121bf3c2262ba87a40":0

AES-GCM
NIST Validation (AES-128,128,1024,0,104) #2
depends_on:MBEDTLS_AES_C

gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"ce1407f666f2aa142ed4ef50eb2a4f64":"585fc1e86809247826f87424741f6ce2ce7c7228fb960803be643acd28332b2036715e2b639fe3f8de7e43e88bd8e65a6e2259391360aaf534ae7566cbd2b3961c874d08636fca117d4123b3063931d7a161d00220014339ae9f447f31b8a2d7d5466fb1ff2508397b5fa71f9b4cd278c541442a052ae4367889deaed4095127":"1225a2662d6652e3d4e9c5556bc54af4":"":"8bc13cc1cb52fbd15390cb5663ce3111c3fb943f8ed3c4f07b7aeb723649fccb90895999ec5dbdb69712d8e34ae3f325fefa49ecc7c074de8bb2ea01fa0554d7adbf49498f2f6e78aa0cd24620bab0f11bf9b2c73ad0eff780eb6c03ee9c4538952af754c566aba7c717d1ee6ac2f5ffe21dab9afd649cd65313ee686596fef0":104:"9a1f1137f9ed217815551657bf":0

AES-GCM NIST Validation
(AES-128,128,1024,0,96) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"5ecea1da76d6df90fd0d4077ef631b17":"d87e9a0c6a9796d60ed78924f7a8c408d5b9fab03fc76790e74029f13358fcae0035bd971a400845f508c2c2cdc3949be498193afcca6d75f8d21521ac673bd41a936a133fb5ed61098f3cb89df5234c5ca5ad3dbbe488243d282412844df0d816c430de3280ab0680a2a5629dce53f94e8eb60b790f438a70fafb8a3ed78a1b":"7d7ae2ed1cfc972f60122dec79ff06fc":"":"1eb19da71857854420c0b171f1f0714972fe7090db125d509aff6d92e5192353187f0906e3e8187f73709d1a60e074af01e83d1306d582a82edbdbebc797a733d72e2d4208675ef98ea4eaaddae2292e336fcd3fa85cdc577f4b8d3f324f0c5cf3919701208d6978f83466a02ae6cc368f57e18b9ee16e04cf6024b0c7fbad33":96:"f74b3635ec3d755dc6defbd2":0

AES-GCM NIST Validation (AES-128,128,1024,0,96) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"6d6de51c30692d7863482cbbaa5ccbc3":"9f242c230ae44ad91cb0f4fe259684883968f3ca4f57a3e0cc4b03ab063a4eacdf63f9e7900a98073e345d1b497b985887e1ffb5fe7d88cefa57dd41076f2da55ce7ab0899bdc5799b23773f8f7a4dfbf1861cf4de377281fae9763dd4ea8dc7c0d632b874c86ac8e4c90339ec3f14cc51bf9241660ab828605cc602984a0f10":"c6c0fa3da95255af5f15706274fa54ee":"":"55e75daa3df3b13a33f784d5adacb2ff6861cacb297d5eaa61693985b6a0f82e9e0b3a28d10648191c6e62d6260d8a8bb471e6b37aca00dafdb2fb17454660f90c2849a9ad1733d7bc227d962b3cd86ab32d5b031eb2e717e4551cb23d448e06bac7b2a4cadb0886fde472d45de39eca2df474ba79eb58504318207325c81813":96:"8eb9086a53c41c6a67bad490":0

AES-GCM
NIST Validation (AES-128,128,1024,0,96) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"76b7f2307e9cf9221c8f3ff7105327f9":"bc076bfd1ff7a9fb043a371e5af7112bb0c9c442be44ca648567937bcc091c127f02ab70b81ce51b2f7a38954dca3d94b3716c6114f0ba349d6f87f5efd84506ed289dfe8a1277a5d1821c56f9f297cb647cdf36d308e6ad41c55d68a5baaa520d11d18f5ddea061c4b1b1ec162b2d5bcf7c7716235dd31eda3dc3094cb15b26":"3cdaf7932a953999a6ce5c3cbd0df7e8":"":"88c70d3cf5817f9fa669aadf731c0eb03c3d8e552f2dc763001ac94837353ab75b0c6553bb8ba2f83ef0556f73dae78f76bc22de9a9167d7be8e31da6e68b0f0bdf5566059901726b6f2890ac8745ed14f8898a937e7d3e4454246185124f65cebd278f8c11fb0de22da7248f33ef6bb82cb1c08259970714de39ea4114f85af":96:"6006fe48f74f30bc467c7c50":0

AES-GCM
NIST Validation (AES-128,128,1024,0,64) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"bac83044f9d8fefcd24766644317c533":"a72daba9de96bc03b5cd7449c2e97c858385475127b9614e37c197225d5789535b69f9123993c89a4815c1b4393bfe23754ddc6c01fc44cd2009b5f886988dc70a8cebb12664fa4a692db89acb91de6a9eda48542b04459149f59537e703e3e89f6d683ebb797fce3874c819d08676d926bf2da2f83a22449b89e204b5ece58a":"1307cd0e6f9ba5570e9781fca9a4f577":"":"479cdb5f65b9baff52a96c75790e3b7e239125f94525068cd1d73a1b8475080f33451ec83789d7189f5ad6a9130e7aa4df10d71ecabb

5ccd980d84d0fbfb342506edcf7298ccb310c0e297dd443ded77cf1d96fc49055534439f1af583217a5de36e4df036a3b6
40d0212658399b629193080d38aff0d4e8aecd6c8d8f48b44f":64:"ca192f8153aa5fb7":0

AES-GCM NIST Validation (AES-128,128,1024,0,64) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"627776b20ce9bb070a88f1a13d484550":"1da4a24fb12538a
724f62b277410d50e918bd6224d4a61df6fb7734300643198debea71686e018bcd8455c2041265d11f7f5dcec08c31fc9
4784404423bcf1dc8e615227d2b0840be123a1efb8201aaa15254a14a2d76a6ddf536701cb3379d3c6b1b0d689e58961
86c88d4a2c53a70bb422ecc8e0a5c3b9f3d89ce40676e4f9":"57f3f9388ea1e2c1c73f60b7d711f6ea":"":"f8a06eea528d
ad12b11ead51763aa68ca062f9f6c1c1f740fb910974f7ad9d2ac87c16fb74d07c3bd3b45f2e26af417e00416bdfee7ed0
b69274ead70a52201c1fc05937438855f5564ec3e824daa0c59da1aa6f6cb8a44ab5f73d661b219766b80656cd3ff1e2d
6909c6ce91fb14931af8580e859e9d7642678c1c35d9435d4":64:"05b432826dd9b044":0

AES-GCM
NIST Validation (AES-128,128,1024,0,64) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"8954e2c0a7ea80fe3c8e75246f75bdbd":"d77e11a837eff95c7
7dd56e9cd97f0ffcee0adcca4a2203d23ce74c804a75cef1bdd69b16228472a2395118dfce636b8916372d6a24106f9a1
68055c6d4b44264674ce3905b3b30f5108ebf939f3fa8f55c12e001b457b73669acd23c1dcabea05aaba34e2d0f66a4d1
c9162764228ebc4d3974fdb38b1a61a207788c5deb878":"2b5f9420b3c583403d92d76a2dd681c3":"":"35b8a04d655
7426def9915eb798312a7572e040a65990ce15a8a6e5acd6b419c3fa26828b6efd2f1f50f91f672fed0feaa09a6ca6b4844
fac5d3db571db8bbce250086b8c89aa6fa07bdca8dd0e1fe76e0f5a821145bafa11f3a9b0b003ad09de73ad71849ac58f7
fd50851aa0fbbed17d222a0a5607f9f75dd3b0d3fa45a135":64:"96511adc097838e6":0

AES-GCM
NIST Validation (AES-128,128,1024,0,32) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"7d0f9109dd846c47527a429b98d53301":"506efc29c0f0291
0cc9f5b2e677bb811e366b9e4910c00b36e48e5d5b42718f3b6d1a08a2de9c6d4ce44fce00fb7e10cf89396a88bdb38dc
b0dba69449195e19b72ff989666b366f03166dd47cf4c7bf72dba3048fa34329ba86bbbf32934a0992d72c463fffee9465
3379d23b8bb4dff03fd86cfc971a2f7cdb90589bbbcb28":"f58a5bb77f4488ee60dd85ca66fad59a":"":"2e2760c649f17
c1b4ba92b1fc9b78d149a9fc831f0d0fe4125cbfc70d52047f32a7f25c716533d199af77ed05e259cc31d551187dbc2e7d
9e853d5f65ab8a48840f22391072cbe29e8529cd11740f27d11513c68ad41f4acc6fb363428930fe3d7c0e69838759415
6e6cc789d432817c788480f3b31326fa5f034e51d2af8c44":32:"6ced7aac":0

AES-GCM
NIST Validation (AES-128,128,1024,0,32) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"034c805b5e83b59ad9d6a65ade3940a9":"efbec09f8189404f
3dbe569d3bab9b8bfabde419fc80abb3b21a07a5fe42326d23d022406981abd558e94f4debf38f2c34c3c315cb1ae1d5f
2d48eae1335b50af9dd05b60aee724edb7d4e12703d5ec8873c55e3a3d6d8d5e4daddd5240fa3ec2d1f32442ce32cde66
dfac77ed213207dc4838ca9782beb9a98d6dc52838831b":"b0c19448b9f2a818fd21ba6489c34fb0":"":"a45ba5836011
fc65882ba8b1d6bf7b08b17f26b9cd971eece86fbb6aac5cdfd42790a7c7390099b10dee98cb8e4bd8b3ccb3ca5d0b9d0
2f759431de640ad7f5dffb919a8aaa74695f94df8eff4c7cb242d643c55d6f9c8323006f3be595aa8cdbfb0d9260ad2473b
244ca65a5df53d2edd69f47df608e22a68b05623150b5665":32:"43e20e94":0

AES-GCM NIST Validation (AES-128,128,1024,0,32) #2
depends_on:MBEDTLS_AES_C

gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"f3bad89e79691ae72f53964b928a09f3":"01913e4ef10226d8
0c5026ba9243fa41edaf5f5c232d17c034db4c0c8369f48d89a1d58b3b2dda496506c30457365bdd76710173a97022d6
47276a4a8ac73f0e9e211cfd7d64849409ef61cce618675eaffe88b3f14496e5eb013c0f8a122dbf16f2c675edf7f813abe
9c56101e570e208e651fd956e710dc09f13ebd22b81ab":"aabf77116a75046e7ecc51a468aa21fe":"":"f7453670604ff6
287ebdaa35705cf7553410452fdb1129a7fcae92565a4217b0d2927da21f3d1b2bd5ae9b7d4dcc1698fb97fc8b6622ddc
04299fdebaba7f7090917776b86b2af4031fe04fa1b62987fa9ec78fbbc2badc3a31449be3a858ac7f277d331b77c0e9b1
2240bd98488a131dbd275b6a0ce9830ff7301d51921ba85":32:"15852690":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,128) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"839664bb6c352e64714254e4d590fb28":"752c7e877663d10
f90e5c96cce2686f4aa846a12272a0aba399e860f2838827c7c718365e704084fbe1e68adb27ad18e993c800da2e05bcaf
44b651944bde766e7b3ac22f068b525dd0b80b490b3498d7b7199f60faf69fee338087f7a752fb52147034de8922a3ed7
3b512d9c741f7bac1206e9b0871a970271f50688038ab7":"5482db71d85039076a541aaba287e7f7":"4d75a10ff29414
c74d945da046ed45dc02783da28c1ee58b59cbc6f953dd09788b6d513f7366be523e6c2d877c36795942690ce9543050
f7ab6f6f647d262360994f7f892e9f59941a8d440619fda8aa20350be14c13d7924c0451c1489da9a0cafd759c3798776
245170ad88dbceb3cacde6ba122b656601ccb726e99d54115":"c7ee1c32f8bc0181b53ce57f116e863481db6f21666ba
3fa19bd99ce83eee2d573388a0459dfede92e701982a9cc93d697f313062dbea9866526f1d720a128ab97452a35f45863
7116f7d9294ffc76079539061dfeff9642a049db53d89f2480a6d74a05ff25d46d7048cc16d43f7888b5aff9957b5dc828
973afccff63bd42a":128:"63c8aa731a60076725cd5f9973eeadb5":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,128) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"5f2af1b14ca9598c341785189ac6e085":"790bc975865f44e3
a1534e978e90b064530321a2280a9172dc7f3451773b01d4a56c1857ad0474350b945e4f34cd677c22ca89445a564b4
7a8526d31d18160c35d2be1e89428c3593b53877cea0d88d85b2a7ed0552e39a0e96e35ae0384a5d7868243045dcbfc2
45a3eb3ff99f4dd86c0a314f68d1971e773caf9c168b0aa0b":"bbf23307ad2718398b2791c16f69cc45":"26b160695de2
ba40afca6bd93f1c2895f92ca9108847a8ab71ad35cac9f9c9f537ef196c5d41b10e3777c9a02ad3c73cd299a85f60e5d0
2794c3be2643c3e63f105b94d32cb4e3eb131d3f487fa5d1de1a4ad80cad742704ed5c19a7cf4e55531fa0f4e40a4e3808
fb4875b4b5feaf576c46a03013625f04331806149e0f6057":"52c373a15e1bf86edfb4242049f186029b458e156da500c
e7a8fc7a5fd8a526191ac33e6b4b79b36fda160570e2b67d0402a09b03f46c9b17317a04a4b9fbe2ddcfc128bd0e01b0b
e3fe23e51b69c28bcf8725b8e4208aefb1cf34fe91a2bb6d5bef7b936bec624a8f38c9cd4ac51a0187635138d55da1fb17
91adfbf8459d3f":128:"db3bbdf556c9c1be9b750a208fe55c37":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,128) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"02980dff205bfa5b18037486618e1fbd":"f037ae281e45c50c
9fa875f0ec9eb43251d3ae1b6acde27cb5edda7a4e384f50301a68bb6f4caf426adb31457c5eeaa789edc84fd902cb82e0
0dccbebe272d90cf690ca82ee748885f02daf377970e985d55994fa668fc5e3e06763e6829059fe0c3eb67033b3f5223cd
4bb654484c57370d2b856d7117e32ead3d179064315b":"27354e68a004b255a380d8480dc9b19e":"37eed862013684
2938ee3c3c08311d1298d3fd3f0456c056e0851a75d844fe6c61aeb2191c024ffce38686c09ab456f0ec26bd76f935d74
7002af9b47648502713301d5632c2e0d599b95d5543ac1206170ee6c7b365729c4d04ea042f04363857f9b8ea34e54df
89e98fef0df3e67eaf241ed7ebbc7d02931934c14bb7a71ad":"f8090d0a96fc99acb8f82bbbe58343fe227d3f43fceece54
92036b51ac2fa6db4bf8c98bf28b40132b1ab46517d488b147e12ceb5e6b269bb476a648d8a1133d5e97d4f4fbdfa3866
a04948851cfb664f3432de223f3333248a1affa671096708ce6e2c9b4f8e79d44c504ff3cd74e8dffd4ddff490bcba3abffb

ade0a4e209d":128:"b5762b41241cbee4557f4be6d14d55d4":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,120) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"1fc9bcc5aee350f1ef160346b642cc20":"e0fb08cf7dc901bf6
98385a38e1a81acd4118f083e52aa52e1ded16ab1e840cc49fa1ead3292ce21096cc75c89dc3701102b0982fd3a6bfa55
a7799e579aa7336edf365574a904bad924ec080b093a604994db4dcd8323d7d39c3c35750b0741b170481539d225518
71d6a0e2ea17e4bebe8ce19ec3bc3bf4f6edae9cd7ab123":"910a81a5211ce0f542f1183c08ba96a7":"2dcf7492c4539d
6abc3d259ba5970033ebc2e7ddfa1af8be11f81b459d7477f310be2171290bec2f2ae2cc51266f46e98c878dd2444afefd
bdb73a417518f5fd4c116547bf442fa9a8cb2300c5ff563117b2641dcd65018081e62a7ce5c4d822563824e5eafea90cbc
eee788ed44e6c4f23fe8926603a15adfdb556f11a0be9a":"514d27f8413d7ed59d96c14e7e74b9f3d4518486876c469b3
69f8c5734145f4aa52506c8f832d4811e5f981caadedcf09875033c5b28a00f35605d773c7f9e1af7f0c795e3df1fa9b5a5
24f1f753836c1e2dc9edf1602d37ac120f3d8a5c093a5285dbe93957643a65f22995a2782bb455d23318f01bd18ae0d08
13b01d233e5":120:"feb7a25a68b5f68000cf6245056a1f":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,120) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"9cf329dc10bcebb484424c77eb785aa2":"92728a696b07704f
b1deb648c5036a1c8602b4006fb2fd2d401c4b6692e252c7f66918078542cc0b1a97486964276d6e6c77bbb88a9fff028
5aef70783d9f2be3b7b22f8a8c02771492150122fe022722bf64263f5d2406884108d8d608273bc02a9127fe4dbcb321a
c44a7d2090cff7017d59d73ecf927b8b05968675a63ca0":"a430b979168f5df5ba21962d1bd6dd15":"4d94b7650297c6
6b43210c84e6e7b09385117ed8fb91adf643b2339f39a5d8dd0b0d75a793e2a669e42c5ddb0873714e01cb65da9eb73f
d976a49ae9a4762bcbc06be5052f750d110a407764280b510da5fd0fdce969f86ea6bf52ad4fd9e2d81ec5cb84af0a1d40
6504a34c51c751daebb4421fe1994bf6db642e64bd471d9a":"c13dbfc60b34d75f8a84db1f6aa946dbfc19479d639004
50389756cd1ada8f6d2d0776607f7053db6bfa6752c4b8456f0ace314ff3fd4890d6093a4a5d47dd8fbf902e3e3000f5e0
2ba93a00985f29ad651cb697cc061d8f3cc74e6d8d0743a1988947c9dc2305e2b7c5a78b29400d736acc238131700af3
8e72d8c98ba007eb":120:"82f1dd58425eb9821fcf67a6b35206":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,120) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"cf43ff6a1ef35c37862ae3b87171a173":"a1e670b3fd62039cf
29edb61b26555bcd0f9184be4593bf6b20ceab263bdc76cdef34992fe0ce4d43bd93bd979b78bb252c120fbaafe4947fc
0ec05cce4358a5089a841c7476b0ebfca6476e690cb9ee0b73c6700aa82aa8f4050f2c98500052a2d3274b30b0be67549
d756efd163c4369b6df0236d608bfbecd784467db2488":"6c56540b3a9595f3c43f5595ace926bc":"5c0bc6e44362299
642f3756acf09878bb05549eb6cd6c4942d39fe586ceac228d2aa9c92f8393e5017e73ee41002e60aa8b993c48a7638ce
2ae0ae0eaa536bd749b07a8672fc620a5110af61232b6a3d527b36c86637cc1fa92c84008465fd861920884d8a784e194
ec52fcbb767a68ca6fabb64ab0a0d680963140d5cfd9421":"8ad36522e4ad47d4a54c5eae0a8b9ff4911aa5b9b13b88b0
0488a7b678f63cf85945b8d4998d1007e27529b56f50b9e3b373bb6fd861a990514743b9707d535b40d1bdbc3f58a63b
8ca30dd7934ee98ec3325d80afaa37e38b4e82d8851166589027d91347727b314e02ed08a7846e29fcd0c764834d1242
9d9f568b312081f3":120:"f5bf21d5eadeebdef3104d39362b85":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,112) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"a0ec7b0052541d9e9c091fb7fc481409":"5431d93278c35cfc

d7ffa9ce2de5c6b922edffd5055a9eaa5b54cae088db007cf2d28efaf9edd1569341889073e87c0a88462d77016744be62
132fd14a243ed6e30e12cd2f7d08a8daeec161691f3b27d4996df8745d74402ee208e4055615a8cb069d495cf51462264
90ac615d7b17ab39fb4fdd098e4e7ee294d34c1312826":"00e440846db73a490573deaf3728c94f":"a3cfcb832e935eb
5bc3812583b3a1b2e82920c07fda3668a35d939d8f11379bb606d39e6416b2ef336fffb15aec3f47a71e191f4ff6c56ff15
913562619765b26ae094713d60bab6ab82bfc36edaaf8c7ce2cf5906554dcc5933acdb9cb42c1d24718efdc4a09256020
b024b224cfe602772bd688c6c8f1041a46f7ec7d51208":"3b6de52f6e582d317f904ee768895bd4d0790912efcf27b586
51d0eb7eb0b2f07222c6ffe9f7e127d98ccb132025b098a67dc0ec0083235e9f83af1ae1297df4319547cbcb745cebed36
abc1f32a059a05ede6c00e0da097521ead901ad6a73be20018bda4c323faa135169e21581e5106ac20853642e9d6b17f1
dd925c87281":112:"4365847fe0b7b7fbed325953df34":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,112) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"f9ba053776afb01d15915e7f82a04f21":"fb59858421ffbf43d
09415a77320cc9250df861e4414817e7b78cab918fa890ea0400d4237f7ebf522d97318ea79f9979a73970296827a1a96
90a039e6c605a0a3efc0077156e1b15f14d88685833e09f6cd6f783d0f50579de7a30907b9d8efc4c650ec57dbf7b425ff
af9a900ec91087d470409da4d67cae7328c15a5db1fb":"df26b109244f5a808f3ea7137f2f49fa":"b21c8101ac96c41bad
2925b9b6c863f54888f36e4995820ebd51f53e323e46f528d91f4318183be0282312ccde8da075fc2e82041cb41a79e99
33012a4cb6e9f89717444bc734da3b7e40e903e58dd0f38bcb115684227ec533c09a93c89c2c2584bbac83a4648f82b4
c9207f43b61e5ec470602076ed4731756c87d4e0e24af":"2c306fc60bff58308f2b9f08d52369e87119d7f6de2279fcdea
0c46c901c8dc5b4f83578b17a00786014a17d3e380e1af4b9f32fa58b9ac763bdf86ff0c6084afe413a5dcb7617f94d76e
59e370eae4829e69bcb70f10545b04ed5fd137e1159f3961b2c01089ebbe2f16a91c782d4f383fbd4d61b66138319b63d
79ce9fdec3":112:"d6db5aa539a6e2e70885508d637d":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,112) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"fbbc406a669b94374c7970f2ac10c91c":"a9f334d1ae7d2960
f39da4f1df85830d27c0f13fa0bd23d607ace4cf58b359584120e7c90d3062b1b23b1a9e85a740c9063ff80423b584625
7e4426c174e8cd77a3dbcfe12970ebddaaa00a8ffb554b2a80decc81f9917f5a1369e8bf7288ed868457993f480d8aff0b
92b3db2fda233e32fabec1a4514715364d4f70f98d62c":"46152f5a68c03dbe2f28e69f5b52e2fc":"1052f8b2d3e11da5
3ba9efe02ce985098d171dff9b98cbc2f6755fd88214ddb8660225a63a1c8bcaf43ff3930e239824ae8e122068b89d7fe7
3c658ce030cb51dae9836aafb68fad77b1cb5bff8d7d9c920ec449181e10ea643cc73abb9620dbdfa32e06c29cfbd8c7cb
8b1103763616ae6f9b19c4a6e1eed88c3971c4778c2b":"7b16424c508da3fed14bb53462d1805f0f9d09f803d4e166fda
dbac76f9fc566665554317431642f6e527123ea6c1c0ddcf45005213b0f2747321fa112d7b893cdcf4c1a59e8bd1c48b7
d77881c6d79de3d850bce449969305797196d187196d0d81dc3423295f552d3c27d6d70e42c9a1a744a039181e73345
0c9985c94ae94":112:"b51dca8e00988af0987860a663ad":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,104) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"fe96eab10ff48c7942025422583d0377":"194c8bbbfae4a671
386b8cd38f390f46f9df6b8661b470c310921a1c858a938045834bb10380037fbf5f5e00688554537be0fcafe8270b9b5
9068fa056ab1268fc166c2d729243a06650a171c929c7845c85330c04568d62977eedf3b1ba9dca13bdb8f9522817c8c
b99e635e37465ec1c9f6f148d51437aa9f994a62e1bd013":"97ce3f848276783599c6875de324361e":"127628b6dcbce
6fc8a8ef60798eb67b2088415635119697d20bb878c24d9c6f9c29e148521cb5e0feff892c7855d4f1c0bfb32ad334209
76714dce87a0bbc18e4378bd1ef35197d0ca73051148f1199010f63caf122df5f71ad8d9c71df3eb2fbe3b2529d0ba657
570358d3776f687bdb9c96d5e0e9e00c4b42d5d7a268d6a08":"12495120056ca3cac70d583603a476821bac6c57c973

3b81cfb83538dc9e850f8bdf46065069591c23ebcbc6d1e2523375fb7efc80c09507fa25477ed07cee54fc4eb90168b3ef
988f651fc40652474a644b1b311decf899660aef2347bb081af48950f06ebf799911e37120de94c55c20e5f0a77119be0
6e2b6e557f872fa0f":104:"6bac793bdc2190a195122c9854":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,104) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"f2956384a65f9627dccf5126141c7bca":"89dfd185bc33adbe
a0c69b55d37087de3fa7fd69a9fa76aa1568ac363c5f212ae92d202b9338ef397266dd8bd1ef36cab6d1368feafec69a4e
3e11e1bf1beba35d96e040d91e9d3a838966bae62a15b18d621f33efd9ec511de4bd287c722cd39b4ba43e7a6f8c8ab67
2d69eac6b21a8d3544ab1d64f9de31956b93b1104431e":"2f61f76bcf074a3d02f51816c0411052":"bde1508823be798
4d5921db4cab1ed3017c0d73cb9bff9874f39a6f5bc449719c1c43d8fb4e76f6813b0985d4b124517f9e4e2d3c552b2f7
5876563c93a44c18fb6523ee732ea5b6d13417db45120653df3820a32ebdb42d544768461b1d0b55b46b09f688e4724
0880930fca7097ddfae35f854891e21891dbad13f661a2534":"023a9c3ab3ed0181ec8926e4bfbc0fa63e38ec8980eabd
2ed75e29b681b3ec04cc8b27fad3a7ce6dc1efd680479a78f02de7ba92f45dc03de02852a2e67b35bb1dd154568df7acf
59081dfc05aca02c0aa9f3f7b4fd4dbdb671b1b973a48af0c325a23467ba5cb59183540f6edf4c00376be39a3a672feb9e
795d1bda96f0017":104:"613eeca3decbe09e977e0beeda":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,104) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"2e9bb30ea25f50b3e7711fac05f9d44a":"17a52f4faa608dc98
53d4511feb3dd9d2fb92d7a3deb3f8a7a6df3fa2a909b7db30babef12d9da71aadfad16bfd2bcb5706ef2addc58eeb8d8d
13f31326f7ab1d0aabfe5525014f05cd8fb80e1ecb0654e62078440157df66f618f078cdf2b322b0f8878bcd924609c33e
42059aa69fe0ddca659aea42ab907b483aa55aacc63":"9668e8b1ce9623ad52468431dfbed632":"f776c6e892e373ec86
ccf706704d47cd89fa45c2abdeb0f9f6f32cde88c22f001150cc66f0fd83e9b75b97bceb98913cf143cd8a68bf06e112503
1e3e7f09dfefbcaef4f04d7bf28aca1992a7e4228fd4017a5b32fc48101c8f5a609eaee9489d02200e8a13efeda60b57df5
3ccf2fe26309a1c1e1d40db6eb8431dbfe8d43ea":"407171db1dfb7ff20d5c97407375574220534ef75ba18dc616400e5
e967e72db23783a6eb9506b611d0c67a83f5c423380ceae66d5dcdffc31e31239357b91794018e9c4c36c286f7b17ee91
1136d9cacf564baf5f9b9831779375e63aaade8734a91bd4000e53e5e412b3f92f8b68e0b7ad3bf6f274744e2c5a63589
4bf918e":104:"2741ebc33a4d4c156c21385a23":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,96) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"aa705ee70297e9212f70585d92f42aa4":"5e4b47d986d55f49
708cb3e4d27072a7e850936b27b24723856acec7b2e03caccd98c2a002a2dd1d3f4dad8827a5910b42986cb00be7bff4
7eb401be5f324cd2cd3ea2fa41f4ef61f9771a4c0184d85d6023f37f3f54bb9d7cd621fe36ce11a82678a0754a33049106
be597c53f287692ac5a42e59f09a2a117fad6c034a91b9":"89822c9db69229d1e4880afd19965908":"fdd655584a92e2
9a14a368f28a73f9dc608e5c2ffd308d4aeff7326bbef5ea58f84620c9ad43c0b598c271527ae60dae6db4ffd3f590e503a
e7057d8c48e9b1bd8f8a8832629bbfc1391b954a4fcee77d40096eb5dcec5e0439375ed455378d716ee8f8b04ccde3291
e580068dd7dbef4ba3685b51940471f24859f8e93b659b":"0f34bb4e2a4016ba41eb23e7688edd455f2d46a5097236d9
a124ae0bd47349876319976aa4c3aa41680a63cea85f433e3a1b4376f79d004710d486a3fb5afbb7db2c41aca400e04f7
5ba91660bb68354029defeaae1853447f8fa0d470b25371da73c9e8ee841ba95fc273f88c2e4604ff29a131a7d73e60a00
340e886df5359":96:"a247e88acbd4e354d7c8a80d":0

AES-GCM

NIST Validation (AES-128,128,1024,1024,96) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"ddeec78a0c23e8c5c32d3d4f9830f927":"134fd6be1a934053a539398aeaf5d3aceda3ef722a6b3568af6958a4b1207f7e9b9e835cfd46a7f3d4faed829ad23554fc7c0d1a9b32bad9477d9dd397a259cfb0bea30268aba7b8cf4a35dbf99a6b2ca968649847f717749bc5f41374e1574ad6c357f7b60b0cffcb822bd3924208d0472a973ae97550b921338792ca88fde6":"ae428ebb974ccfbbdbcf6203105724f1":"e3d5ce768c688e881e72f036341b2d91947e02b7327eb53240c85b0b93a40eb0f3346817e2c9e126209b31b57633c4384f7af46846d9bbe6fd0d6babc57b84d0f5be2a8a7b146b38914a4cea70273d5461126cfd7527ab397510176e790300a06066655907d499bded79f5bb39f6fdb03f85a415c2cc2ad1f25078f0da7df215":"865d6148c9820b67c08c17c9214de612ada6e24ed67933d13c3b3ec43637fa305673d8d52d15a195b27a6b2563682a9f98912908668e3335192b1daabf26e1e73d7d34764af006b0c14a0ffad3b6a0def59964b11eb52e829ad790069997931d09be88b8d60aef90e39dfcb0df4fd54b71597b8ac64670e703e7cb83efa3f2cb":96:"64b2458a6eaa6f12937a8643":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,96) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"829008339e983918b8d142091f84ee28":"6f30604d8c2fae216b1ed3d67485631eaada68fe89a7020d6e29f42b937e7640fc1f23c00ba48bf239740f6468289ed211ba81e809cda55fe067bdfa198bf0461daf86d4a7969de9a629513809b358630ce7eb50a783b8c98ec1bd5e56cb47032ee8fc64a939dfc4a870ea9419b16178109f1966ab964da34debcf00cc49f57e":"dc62cf12b6d0439578b457e516d8205e":"e700cd917923b16c968712b2fdbf08be1b5c3b5d9e42cc45465549898daa07c44b4cd321ba16a38aeb6720e217a58428e3a4cc125920cb3fc92f039b66716543bab71b64ebedbb1e5e3e8fbbecff3385ab0ab16b7f6554b7fbb3b4c92307c654361f984d5a6cb69b8708684d90bb1fdfabc0cb59f42c2b3707b3755a8c7abf34":"adf60c4affb2ac76cce20cf9f302b909bfda1bedc60be21b53f65d0b81bff08f7e90ecaaf12ee1f9d921926b75e244b7e8357c1cfc26013a6d1c874ed2e5cd0cce012bbfff0dff85b372d92c18dce887c1651b6467f173a67ac8cea194a6c41e77842675f60cacfbc9c81597a08959d19af632d3c191bf69505620e4290bb040":96:"6209c09dd1b7ea85d02eb9fb":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,64) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"4aec55c7e4bb36c32cb543b57cfba3fc":"4cf1443a5448fd09e09e91b7cc5f8e00f53f0b75a6b17db5ab9a721167de5f7bc5de1fb711accdafb7f3f1bf6b98393e5f09e9091e26d1340122edc91f7e60f62caa218f1927c8f0032be0752520aa650f6f1ddf40412c96d49dcc2287ee17834504f1dda3f4a723e2fce064f0b8dae0789ec455922a14488623e3ac10b6e312":"6669c3022e0820634a95efa2b5578e93":"f6ae9b1aaba18acb741c9fc64cfba3841f5127b1cda5cbcd48af5987428daa5782d2676bc3e2ef23936ec29a80d6b5310282b39b77181dc680799ac9c8125fc48afd185cba2ca8900bd9a0039787b4f3a6846f3edf5f7b921dec2608fd3df67600ae0aba9378da0015bd57d66d2999bf751806d1b89214332bac50f721ca9474":"720c32b0d454f086af36a32cc7274e2f2fe08db9cf1cefecc14b42b3e5c573aefa7e9e1ee0042eee21104dc3e4d19b012099280c5a53e40a0bf662d8295dde743143a28be7305729767a37cbdf08fb3c87667939a8ffe44c96ad272e30b75aafada2963bb9636f189c37d976ed1c458295fe85ed19662c463d7c8155e9f04115":64:"4b3343b627095f60":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,64) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"8629e8064b3ba2b95bc20dd075f8e931":"85896de4b6454acf8568ccf95ab68a632330ce71ca8b4e7bfe26ad8d7e2e6b63f2032e2cd365999ffd24ece0df16904d749d06e829a291f3d07fccee27d9c6f3ff3a139d9e33f0660803de8fe79dc6ad291fad47c93543522a1c38e40697426a9855255e3e0abcb84d474ead15341c6b235ccd755e58fe6e87898d216d65abac":"dc4bcefe284cfc606f39b057b7df411b":"abfd0cb6fee8588aa

68606b7e487bb9c0d2bd11205611a6f30a78d9ccf28e827cef4e966fa245e4b7b39533a4bd00176ce3c97858b0c8abdff
4c548c835bf1962a6115c4ce7c05b1ce5aa29b412e816abc925b8cb998eb4b69c43a7dda1b3cf0d728072d42cb5a489d
b521698c5daffc3013537bbf622ef76a2e96089b7d4b96":"b295ca0d7707892fb08537f42d28a844f5877177f136b4620
f69b05c83f43bf2e61323e80076c88660f5385060228bdb91d866686e691cc7e96fdaff41f2ca5f5b5d93ecec7bba82515
a6e0bd604c99ef93d3ea013d899464558bc822bd765eb1ca2b8b8a7d961a6a316bf135c22d2ee552e62d8bbc5b60ca31
bb53cde82fb5f":64:"d26cba11f68a5e1a":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,64) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"4d901e59a491c86bf538f7b38247bb21":"4c370a9f316d257
02195409d8e73bbfa40aa15c2b0ea55db9257a9ae4e8dccad14589718741a78e5a74c26a801857e388c9f141ef7df08bc
01384b2b2338c38abce51d547056f4bbaf7484f9edc96df122e71f132b7bcb6484228c3ae2f741a2c8b9b208b6f49b070
81334b93c501938808cdbd2e40cf95ae4f27a29e1121480":"39e2788c9697e82cae0e222a9e413d8f":"48d7d20e424df
3c3efced29e860771647ae01312a96e68d33f982c540e74160a7fbdb623d4b19abb1871d74c6dadc56038954b154389b
752bebc40cf4ee1505ec8d844e1a04dcae430befdb081cc84252e0840f5f5146ffe5b9594f856afc2edb33b3c6f9041c963
1c5e3d812959c5504938635f72c6fe29a25bbf66a4ecd211":"262718671dd0e2c9a40b9d7297c7f6a26cd5fe4f301999a
32059812719896d3a2f5350f6ec20d999fc80b8d7af5a421545b325de9180f14505f0c72250658a5014768fed63ab553d
e0fb01ab1368356043f6d1a6c9950c80e3d9d4637bbeea44c9d58a4148bb10974d507c62b67cc4e37eaebd7eb8e67077
856cc5d1702f8e2d":64:"bd814b4584941681":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,32) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"2f54229167862034ef6c5ff4a1246697":"af2c89d360032977
9abfbcf5be8bb83c357d4d2435fc8f4c413b956b898d22a8a889db9e2ff5e7229d7495576989695a0b52d796f9a23e957
0b7caec6b46059749c29a293d31a6224baaf73711bc0e4a587abe9d0379adec6de04ce444676dfd8672e6660cfc79d7ee
2e7625ce57dd4681bad66aa29bea2baf936122c3db17e7":"8168ef8ef278c832fc0ec846bc9f62e9":"abb9ed241379152
65bddbd4b63f1d02efa2a99c8c373f19077c7e1c389feae36a7af42c661b0adc5dc8e4b5520d334e8e0e112d42c2977fa2
3485c0a85aef83f1e52d6749bd29cbebe14aea6ee1c1098aa96c6360b0192894bb2001c7c0fed7f00bb84953c23bfdda0
0818d1568fb94c1bd971982d6c01c12a35ef7af34f947f":"cd6dede25433fd3da6137001219b57aa54bdf6039a5a8d661
38171b006194fe3e13d484e5cf57a1acdaa8e76f001df7bf41cbed2c5561a37a32113fa116d0918167c29dd9e7d46f7c18
d9db33d7f1bc33ac21d159ddec57a2e158f0c0993c16dbf50582371100a8d7c55cd47c03473c5770ad562240f754c99d
95ec593dca284":32:"4ab63349":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,32) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"b7b52fe74c5c3266edf731578d28a72e":"01a4b7da57c0f7d9
aea51283004b23f899669dccd6dbaec9cd6e747c7adb52432c7c29d1411ec1df4e5e33311ad84218075dabe17f73c9551
1ce7950f08b618feff56bd452b33455a1a03caa8371dc7fb9aebedb3cb652d94e06bd00a98bb06d30b506d41cb516c759
f6d7f793472e6d6dc9ae50cf3dc8b1ad3d0517c4f555a3":"a005750e9f8c68ae238668f0a8f015ba":"805cf3635f9d84c7
608c242ee23a4837dd3f260de9afd6166b08164a0256200be9b52e5259a4a54186ec067ddfad90f5c4f92afd1c7e4f2d8
443312ba3c4818b664439a02644e55467045071aa2cc7939a940e89cc52c8a53623bc6473bf843a4e0f00149b2ce1543
a6540aa0d9c2c5b68ba2bd5791078deed1de3b5f48257c5":"d6124da0896d99fc7f2c3688fbca164f8fecd75b6260162c
4dc2d2773ce75cf41a8c7a57998e0a7e49cc71e5ad6a04c7415f8d4fd11f1035d3a02ed744345d74ebc9c4f202f65bfa88
d55c747fe777225e218f2149da22b53e6584823dbda42cc2dda56fc72b753f3923c443eb5c656515dd824d8c08cc7815
2226ed8c1808db":32:"60d86287":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,32) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"7a3501d9fbb86ab80f5faeaf8876b7c1":"4f0dfbd2aeab70c80814a1f261a1fe442eacff5d267fd0c0f93757919810f6610113f1b442270afcc47f2fa01ab01797683ec9267691a0dec45033c57f5cbdfcafdf154fc99e6140176eea92503b3f6fee5dfa5aad05f802e08a08f10e49a8b32a50c028f2bc7aa451be3747d10b96b3a1105c67c5167eccdc18b4a9b0612d03":"6d59be1833e75ce7f54ddc91ad6f5187":"3e556b1b33c42f1ad6cca67dabc6ff79d6cb667527335858e26cb4f6a3d8503ec415968ba97d2d79a3f80c1a10d75174eb5294cce8b89224eba7dfb258fb17cb5c5db7a914ace06e94cd2f2cafe3febc8adc4c2264afa2db2c6356e4c3e8667393a77a0afc36be678d5c0a4b63ae82d9922bbbc60559f331ece9947b67469469":"615ea4535f1e579d7aa45c011018f272c2e234c3ea9e2d102cfaa4a437c41e64bdef7a211ea4d858bdb656215e600911435ef9c8da68e8239e4782ced7e7add063f33f5bc62b85d9ae44ed1b139580118c5fc054ead08257b0a97632e8c503c6219294af423f0deb36758e05857ebb05c6835972488306ebfedd2ca4ce3b2c48":32:"74c6bf0e":0

AES-GCM
NIST Validation (AES-128,128,0,0,128) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"195ddad2b0da195ea54a9dad0f86c161":"":"265ab1995fac4fca7c2b26c84e4a2dbc":"":"":128:"930f719034b76c232619ef2792fe6e65":0

AES-GCM NIST Validation (AES-128,128,0,0,128) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"12be48e90c849063637b1c2ab0f2b467":"":"0020c3dff2f6f3acaaae982ce38f63c3":"":"":128:"c8891f32b8015024ca42536d633b1863":0

AES-GCM
NIST Validation (AES-128,128,0,0,128) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"8e792fc91675d5efd4d80d5a06378d24":"":"15ad63b969f8e313eac3c717ff9a994d":"":"":128:"de9a04b030954b0141dd78ffc67323d6":0

AES-GCM NIST Validation (AES-128,128,0,0,120) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"a668cfd45b6ef8b766a4bb187d0824d1":"":"a111e94a6426ad9b4362132052eadf4a":"":"":120:"3a3331e6a41cada2cca8e856135549":0

AES-GCM NIST Validation (AES-128,128,0,0,120) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"f36e07f2689832b914e0b817010c528c":"":"654104f9d16348231e6ba6fd30c1f02c":"":"":120:"be897583bae073f42138d64e622c35":0

AES-GCM NIST Validation (AES-128,128,0,0,120) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"25d839a709d98ef9c0c9e78ece961eba":"":"b64537609040790ff648d51406710b9a":"":"":120:"4d5854c69cc973be8de41d5584407c":0

AES-GCM

NIST Validation (AES-128,128,0,0,112) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"957dd619f9f19445c374ceda9e9ac082":"":"34887be03b4d4ca8ea2261b600ab0b0e":"":"":112:"60e2d50adff707d8b279bdedb277":0

AES-GCM NIST Validation (AES-128,128,0,0,112) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"a5c9a2dcaf576e67828e806082d8e780":"":"f93732aac9448c4a427e634089d7edcc":"":"":112:"f67ed1c98bd2c5f3a738e75f15ac":0

AES-GCM NIST Validation (AES-128,128,0,0,112) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"0a30a816e8d4d85d40c8e4d7c93b777e":"":"bf1f332aa19682d05cf95f2b03d26af9":"":"":112:"acfb2f7884bc496f3089e50dbf42":0

AES-GCM NIST Validation (AES-128,128,0,0,104) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"b45a16bba5fba362704149dc56ba8a13":"":"64cca850412091bf4e120ccd612df353":"":"":104:"7b1adc23af9be185e5ae0b0f0e":0

AES-GCM NIST Validation (AES-128,128,0,0,104)
#1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"0cbcbc1c72aa90e3ea7e2fe328d79723":"":"2fc5fd964b45082546636ae1e208a937":"":"":104:"fe091a768c731e54e2237bfdc4":0

AES-GCM NIST Validation (AES-128,128,0,0,104) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"94297a1ad3f0c333cd9b087b1efd43c0":"":"52ec9dc82131d7b1c69c01fed6aada10":"":"":104:"5c927dda855b76ab8fc077203b":0

AES-GCM NIST Validation (AES-128,128,0,0,96) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"1e8cf32008bdf867f0ff76e7d7ec21bd":"":"3854b7412de72fefcc4b0c2155f6910e":"":"":96:"cc8e7eccc056b06cffc307e0":0

AES-GCM NIST Validation (AES-128,128,0,0,96) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"2ce1a9bd93fdde2adfd8c2c16a395b95":"":"64072313ed36eef8209f079fa622d7f0":"":"":96:"cd9e8ffc1423270015bf8e8b":0

AES-GCM NIST Validation (AES-128,128,0,0,96) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"b15354ad3d874fe472719ebccd45f123":"":"1b2013153290edef60a6a438bd7517de":"":"":96:"f65a841ed510becf52b1eae7":0

AES-GCM

NIST Validation (AES-128,128,0,0,64) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"14ef129784776647eb3fb8897915ab9e":"":"f7bbe9f699156549935f2b92c1dda163":"":"":64:"dd10fa64fd51231d":0

AES-GCM NIST Validation (AES-128,128,0,0,64) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"5d4470053c46a577bba7000075e9bf2c":"":"854b768fdd7492c21618ca716bc8790d":"":"":64:"1f3c73722006023a":0

AES-GCM NIST Validation (AES-128,128,0,0,64) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"ea87d675a0d406c57f78a2531bfc0c9a":"":"0907503fcb06ee384526f7206180a080":"":"":64:"65d5466392b63bf6":0

AES-GCM NIST Validation (AES-128,128,0,0,32) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"d3e8e27568e6e17ff807cc207e5d4eea":"":"18e51cdfb4a3a5ebc7b0d7b17727aa95":"":"":32:"a7e3f637":0

AES-GCM NIST Validation
(AES-128,128,0,0,32) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"596a602164b1a0bb50ef91bce3a98796":"":"2025e72bd6a511980a8ddce34565d16a":"":"":32:"f84f92de":0

AES-GCM NIST Validation (AES-128,128,0,0,32) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"d0194b6ee68f0ed8adc4b22ed15dbf14":"":"32ea8970a8cb70d6ffb3972a146c6984":"":"":32:"eef4b97a":0

AES-GCM NIST Validation (AES-128,128,0,1024,128) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"869ce65e5e5e12c620076365f149784f":"":"317bf07e83c2e9717880b7d080957fe1":"ee185d738260de67f1792a7d548ea73267fbbb6543bc081fac43e00e6cca92d7d646f27054894664ffdcbe635e34cfa800912b59fdaa624b36c44c9ff4f193d3be2f97a7820a6d4ceabe967091ef672098baf82dd3b671cac4fd4f4b14e4ee388fbdaafb4dab2385df4fca23a78d31f11bca15eedd7cac778484258778106a07":"":128:"add6c89153c4c0eead03df44487742a0":0

AES-GCM NIST Validation (AES-128,128,0,1024,128) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"0a05baee927bf23dd2f4b57b90fb6434":"":"8147e99dc9e462efea9c1d7f30bdf45c":"6424ca7fbf24c6c3b0b5eb9d769b26a9792c96a8585dc596208ae6cfc0b265bd8d26af31027f278bb92a9e3b365beae8d964ec7a4096513f84fa73f8739fa7e11d54d678bed19546d2b71b3d0166b25b47ad7cfa69d74057d889258a796a65f2bf8d3bb151f4e721d398e74594a186e6182c16fe4c8813dfec67215b3c4a94c0":"":128:"05fac5520a99ad7fb407c48995a2c331":0

AES-GCM

NIST Validation (AES-128,128,0,1024,128) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"e28c435211743a7872e4a0bd7602336a":"":"2ddbee94fcbfac
ea080ded468f67180c":"63190ef542656cc2b69a9b0daf8dbd2d38cd75f17b92d6d891c17b0337ad4fe4539d9154722f
a430782a1d79620e974661918166e39c453c5a98759a13d2766138c7750e6cbdc7b6d7cbe44f3f4de7bb562d9bce6e6e
2e815444842b89ba8b73454218c483e574ca886a84e8c9aa6f56dd1541a7e35a4a5b8f6a05ad5bb013e9":"":128:"2ce6
d74cda466354a736636bf18acfc0":0

AES-GCM NIST Validation (AES-128,128,0,1024,120) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"2b2bec16c7d326a35a8e4c0b8c2e3674":"":"4573eb54491ed
91bfa2185b762115bc8":"7a4a6b3114dabc50b201472c5cb13a79430f78eedb2ba8492c01ce10a74d08565b9bf9874bb
8fb72f694a23babdd08684cb68d7e09e65813728aaa5c41f9c2b10d921f8271e200e0c519c7c46f572bc9fe3f27e13d1e6
d7bda4bd66c1c4b0fec8c68a1b0ed7b0659009dc894ad55e0712ddd0837315734f2bc3b757241af35ba":"":120:"5f5d4
695795b8580b0bc414a81b002":0

AES-GCM
NIST Validation (AES-128,128,0,1024,120) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"886fb12554b075dd9663efd076acbe56":"":"7e7a73542868f
c27a01865c3aa635ad5":"cb25c2f029c7a877a0aa565c7f7347b317ad534821edeeea838996dfc42b13787e5bb237525
ac926ca8a6c5078210f4a27863e8114c728d09653fa93ae990e99f0c856bc8097c2cd33cdca1a407897e2f495d2e75356
aabd891702f25ff20e6b6c8a785d74b78a734e311fd236f9e970202674004ee4151879d59340b20aa23b":"":120:"8255
116ee1e3cf936633017c4dec3a":0

AES-GCM NIST Validation (AES-128,128,0,1024,120) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"920fdf4b39c63947d57a07eabbf3f2f5":"":"77431ebaad53e4
2ca7eead0d45e5bd18":"11f82f9ef7c2161ba73cf7da82c5397da5e8278da180a976f43222402e983b057171f793641a8
343d6366d6cc9260dfe8becb8396b5bcfa0f46908bd809bdab61126cbb8d63f601965fb9e4b3afd66c594dfd394d4cf06f
79f361771a85dcead6f45dc7df10fa434736eb109a76fe6cda32c5773d4db6449494f2a3f6c884bfe":"":120:"1291cbea1
a9f8b166c7306ff9eb281":0

AES-GCM
NIST Validation (AES-128,128,0,1024,112) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"114060534f526895f30dfb4007356ea7":"":"5ed7fb59618ec3
d081e60d8259a3f184":"a56566a98d9d4fdcebc932adc405e0b8190d537f931983168283d0431e7589333d42f2a3d6e4
1f268e7b566cf48694cdcfe01fbb9198804ad39e7d387039575c5de787610a23ec265505a448c3a64ddac1b0d8c567eef
e5c3c2dc1bb15af45b4bd8fc2e1506ddeb2e39e04f72fd24a64cbbbc929800e0687b53eb89b3049f271":"":112:"62f770
b3985388ac37e14e8d4696":0

AES-GCM NIST Validation (AES-128,128,0,1024,112) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"697ca4e9de580b525d7149e8b69e8093":"":"e844153734eae
bd86983aa3bf50068df":"cedcd5ffeb7988837c38a0be4234ab1b03f14367a1a3854b6dc9f33eb9a87c411326e5cb7d12
dc730cb6f363da2ba68affdfb651fe497942e0dd59668f56c23dae80b7bbf905d36b501ff037fcdffa472efa4bcc1c975b6
7e5d7f348db73e0ce648b44ecc5b5bbbdf3101bf32ea99e3c8e8991c94fa609c93d4b375a4389023b":"":112:"95becb04

cd39c868c9dbd1d4e59b":0

AES-GCM
NIST Validation (AES-128,128,0,1024,112) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"2fa92cc97ef469efeb2c25838193435a":"":"07e6492f2377c0
4a85045d24940fbe8f":"0f021fb787c6de2be054bdb2741aef82ce35d951de2986c86c3dac77ee0804dfbd010d33a5dcc
109769d4b8ff1471eb98fe917c7b0b374e80539f2f4432f92aa55d8398a71510c2acf85c54975fb09ff5638b936283efa3
c1d3b054865f97685d6bfa0dfcffde3a20525b5324573b69dde230ea87c685e4f6b5c3c4c55828a86":"":112:"397b2b0d
ad7f1926bfc25a3ba0ca":0

AES-GCM NIST Validation (AES-128,128,0,1024,104) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"a61f8a5777ec3da0c3e257d421286696":"":"14894cc4ff71e2
49f0053bbc1680331f":"9df46dde257054160854248e70625183bf957ecec36fa4f5a79a1650e04b500f7f2fab4bb873f0
e813f0d6b17610bde0de95427a8e2d1293dcdde053f5b1a5a81af25d553289e89e77e4ad7d0a1190151724730149050b
d021ec61a08ce2271390161c752df8b5f61c33ee39366de4c1db41d085ab9dd88e170e8c41c571e2cf":"":104:"e062ab
7984221ed226be353731":0

AES-GCM
NIST Validation (AES-128,128,0,1024,104) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"aa2d04f4f5258c6363b1210c91aff7d1":"":"6b24c03273dcfd
508cead2df0c65ef2d":"81a1b326f8f22bfecdf1f386bf8fe678a427e3886801b823a37860b9a832356724b1d352d6250
cf8e8f89d0bf2314fd11464c3b4871478f0bc290ee1096c8f6cb5484176d70762289b44309d6a88e4750185abf30901bc
f8d952da9abaaf9807c0c0ee8be2b247dbbfd182b83f9bfa67ca3bf448c3f5a3de3c31b058c3f944a9":"":104:"80dee09fe
d5183d6405beeb268":0

AES-GCM NIST Validation (AES-128,128,0,1024,104) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"cf221e6cade9f6cf509afa6979cc1fb9":"":"d35433be41a259d
faf58aac1d82af462":"b31c477490e5624c4aac8e590725bfa8b3efca618e2369e9b980d6a463a014d55aa8317a9e70ce
6de7c574cd15242cf4eb3eb078cd2f49fd82d1a56c6c4241342e62a2e9d94f0aaa024055cb441d650f0a6ecabfe9ef563d
6bd87d4cb1bed348aee42487c13b73e52fb70f0ca6ed81924fd519806e04babfd08df1a00191caa1":"":104:"f1776b1ee
7a3c49f99f34f582d":0

AES-GCM
NIST Validation (AES-128,128,0,1024,96) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"c98eb634c7caf52d3f3d9f344e141988":"":"a0e58176826910
a69c2d68ae1c6a05c0":"6e559278bc469cc670c4d9105c3c2f8fa308e11b4a60f75664a9bfaff4f0176175ddd3c6c17ff9
1a208dbbc7c49efff099fa873f60849ffaa3a3003419cadaa06b92a678b80bf6c952bbbe596dd0a2eed35507c55c48a9e6
131bcbda0621cff87e02be5d082944f2c8e27211527717272839601b0e26cb5aa2301afd05ae1b35":"":96:"3d8617b2d
b536ba7d367013c":0

AES-GCM NIST Validation (AES-128,128,0,1024,96) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"c5018f4a8e2a850979b006d0498dd0fe":"":"75e4bebdd1701

59cff59f895ebdeb118":"25ed2831fef205690381c73e925ef7ba20d5f2e3a4b5d7beabd749fafa08a6941acb1385aed97
7ea824322d378649f646a812e6c87ded6ae437c68ffdd4fae937a8498ae825d7523746730af84d56380be8f575c60e7f8
36a862343916e98cc2aa5a27cd63cd92df63b8bb47c81fa6a53740a125bb9cbb247c916363e60f5f65":"":96:"0aa5aced
93e0237bea9a0015":0

AES-GCM
NIST Validation (AES-128,128,0,1024,96) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"cefd40aeac28fbea6e3343a125fe1c9a":"":"324b9722166edc
3831bd19c1db5bfbf2":"72b7a4289bf7f5a752665839adde8f79644424839db059ce40de326414c09691d5c7071e4372
2104a94e430e263bc974b98f167c50b97490bcd4286b502f607ddcec5387695463154bd9598ce8ffb6104d1f7010bc19
6ea2dcbfbf452d6257b1da00271fe1e6fb56c43656d5570b965e0369502443536cc46d4c05b1e863ed8f":"":96:"0c6b2
8de22e02fe6a4595d5f":0

AES-GCM NIST Validation (AES-128,128,0,1024,64) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"58cb7cb58518ff3fecea4b44ad9fdef1":"":"fe619efb1c9502c
03cb8a70792f9e046":"1a7c444a84267f52c36f3c09f8c4a88b6ffe3309b8edaad93a08d3961af28b7c2baba5165f0a9ef
e13fa6a0ac595da156741dc7f728c11edbd8ab02f03e45716be504778a75374ee882af488bfbc6cdd58fd81d3ac5f369f8
5ba42c6fd7f9df4b25fdd2fd32607ea800047e06058388c4f71a5eb4d825e8578106041c84c25a1":"":64:"8243f32002d
33cdd":0

AES-GCM
NIST Validation (AES-128,128,0,1024,64) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"15cc4cb979a343f4adfb821d6f6e9c66":"":"68464e7eb64360
c7c0a8540ac3473513":"d69f4a9595a48a50ec33ac1848df3d994eff838b28ea7c8b2c42876dadd60a3f9769bd4f61d80
07c9dd4fde55edcec8f5ac3bf23b1a958fa714dd88cd5261edb69b7b086ef0f442179943f0871a6253aae99d31fdca448b
c3efef353b5cc55cfc576e4a7fb73a5ab6b5af58dbd381bf7f9d69a5c2bfc902901fd485967b23bd9":"":64:"c0f4302d82
76c3d3":0

AES-GCM NIST Validation (AES-128,128,0,1024,64) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"6398de910ff8f3acdc2217811a1da2a1":"":"fc69b21ec18195
901ffa62260fa20454":"021f225240cc9a68c4886824d373f3a70fa32b3a926c78164642450287d269d39dbd49c8c71c
e7b914f83e8b53bc61c6773f98318557b45f0cc2ef2539939df7a1e6765117f75631dc5640291d20e6402d22cd2e231f9
c2c67cb24ab5d8a69933c49b89c9fb2ea57136a6bf1bffe8e04d8d6c813040215f051c654d93224edfc":"":64:"314d1a3
32d3c590b":0

AES-GCM
NIST Validation (AES-128,128,0,1024,32) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"382d86868ccd08d417d94f3b73729e09":"":"069069c37795
8235171437b34e0fce76":"049af372e34ef7a92d0d49cf2dd03052dabacf2982eae6a817e6146ad799971be239ef5810e
c3f6cc6990e9641a7b696392ad3faee38bb50746c1e93913c02dbbcbc6bf54f0d062f176779b7c0dd5d7ec7752601c981
2fa80508a78bbd26922bed4f64b1ff2a8340ce1c01e317e3526cd8218ac24af87b07f8792849f6479b8e":"":32:"ffa59fa
2":0

AES-GCM NIST Validation (AES-128,128,0,1024,32) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"21052b2fc7bc7a662aa9dc4b6a04f25d":"":"d7e5432def6a24d486a608e5c5c919a8":"1970ed40003bccabf7f3c57bbe5ba27e4254c1511413ed421cef3a6ffb9f0192987de83ae965478c3e9979637f8b3fa5d10d69b916f03fdc92ace7736f171660156d880114aefdcc164adb6f8c03940d9b43ce8881441b41cafee3351a56fcb632aa4b09ea81adea26fb0d8c6e1ae380df922a429ae1f5b82b38d9bda4323c51":"":32:"ff342f4b":0

AES-GCM
NIST Validation (AES-128,128,0,1024,32) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"b6c53aa91a115db64653016375bd747e":"":"8163a4fd9c2c7010bc85c86177b194ab":"93cddd318b999262c7cde2838cb5c4d78f3eb1e78d305e5f808fa5613526d724e84a0188ff42a2c34bdf3b5fff70e82b3c30346e179fb3faf378bc4e207e335a44da53a5ae33770104b95397fb5acb746e6418d0dfc7368b035af53b470fc66bd0c210b68ce1b276820b621e919f044e5cff5ced7e07dbb8825bca6b4ddd8ee2":"":32:"50b8acce":0

AES-GCM NIST Validation (AES-128,128,1024,0,128) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"2251815f5bdfe1111c7f9ca246662f93":"2247e781763edb1349db2cda53e5853b726c697b34497761373c3b6a1c44939207e570e14ea94bd5f9bf9b79de9cafedeabc9241e9147453648071f2240e10488c6e3d7077750a6f7ede235d44c5a96392778ec51f8aeb1a17fabe9b6c95fbc479fff954a676813ad3d2f71c76b9d096a0527f2e1b151aa8972147582c0fd2bf":"58973280c2a7122ddfcb25eb33e7270c":"":"b202eb243338849600e2feba7f25a05fe98323bd7cb721ac49d5a8136422564391462439fd92caad95fc8cdcaa9a797e1df3ef6ba7af6c761ceaf8922436dd5c8b1b257f801c40914c1331deb274c58eed102fd5fa63161c697e63dc9dfe60bd83cea885d241983a7e5f0d6a8fd02762084d52bf88ec35f156934e53dffc0395":128:"c3701ce3284d08145ad8c6d48e4ced8c":0

AES-GCM
NIST Validation (AES-128,128,1024,0,128) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"3199b70e7115c74e3aa3745c18fce8d1":"4fa0b090652d5a8dcd9b5f2ceaaa2dc87a40b30e2d59bdff09e1f204d1b90371de70935c385cf5b4d7e0c4e88661f418705370b901b97bf199b366e669bc727882d4aedf8171a8c39431f11af830358cd0d9e110da1a0cc6ef70efb255efdac1dc61e722a2d8b7fb4cd752c6350d558ae1ccd1c89f8ba44ab697df96681ee301":"808a019f7fb761e9701c0c4f1a1690e4":"":"8d5ed4146fb491db9456e92f753aa4f688a9bc276e6aebb782a0cdf7fe578d74ca3946fa7b7893eff6345e64251cb1b146442acb64041324e2847481fd4388b17f83206948e67c1e66b894d5d40ecac0bbe4db0c6f58b65a1f19f29429a9e76f78ef5dba0c94d88dfc06e6222a506f004d24cdb3fe26d6eb6e08e4fdf6289651":128:"908806d668451d849ba0268523eb0e4a":0

AES-GCM
NIST Validation (AES-128,128,1024,0,128) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"63805cef84ca7fcf281b226c3ae37230":"543fd64d1454ef6c007ee96b3ff5d2e4b7f5d15c23e7548dfd1dfad4da7774b8795e817fab3be7fbf8e4d0d351a743ea793d9d01385a552f78ede054be079aebd1511013de2096456e9fc1b83457fa1240cd39c17440d4b55c4e390119a759055ac851a02ea481eb83e294922d35f687a56d801eed638d289350e141116ffba8":"1aa9e75d7854509a85d995ee482b8eca":"":"98db9e8e3ff23f09e585e5326f525e4f8350a1f233a0aebd60d5951583eaf5220f1690ee3607ba98cf8cc99a90efb7197835957f2bda918a32e528f55d548e3c83d65910b956634224cd5415ff0332c165d1241f7a93976649ebed2cc7e62addb76231bb738ee8a291b62365965392aeb72acc5f0fbd2f88f5613fcf44a1b074":128:"9b1baa0b318e1f6e953a9f90b21cd914":0

AES-GCM NIST Validation (AES-128,128,1024,0,120) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"2ec9245e8f567e1cc8795bbf72f2999b":"f266d0060d290339def5f6d8dbf7d120a4c645aa90470e168b4f35342a00b8c7b7230003657d377d8568d252765df142e97a9dbfb9711d9ccf396f3d51bd91673f129d58efd80ab83a0678303e29a0dbeb1fa9fdb7fbde586a17ace65e894374ec8da1ccd3e21851ab998534de46cb43b38e241edc04b5c571dfc0aa0074d4fa":"413628d9ff3e4067d840b0abc2cda0eb":"":"145d83092a269c8afea604e9192b8bb550b9bea85f842fcc4997c2b00c6f3ca46100e814e82389f27a69a12d29340c5827e607657a00fc72c4de30079e23760769e800ee4ce46957f82d61935d07d1c70dca836c19969dfd0fe0ea740a52e2d09b1c9aa137b5e8527756fb2c2298f8400949ba24a8351c1093626723a68a79f5":120:"ad174d1edc713c187a5859a390fff8":0

AES-GCM
NIST Validation (AES-128,128,1024,0,120) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"b08df4acd253f9dd4abc52c4be488015":"82f665910d853fd2b775bf66a1707935443574c90483fc33ba02d6479fafd99c5f816bc58a1393a44fb32711fbeb0d6936efeb3580f147c3019e9f2e2ef48b202bdd369c277791bce524f3b22ceb74c664143c4b1da819b229a5b480aa954be110ca006615d9cff5a158342a47cb6d04fbb817ae4ddff6d4f86b74205799c9c0":"e1c27d35520ea527f9a2cd9b0f717841":"":"f5b0fcd812061be999901595b3547e70f7144cc9e0b0098262be4c440e8637af782f536f571534a658ad1fb44360d9c454d1000d6957f261401e09c0f19f5146ee5433e378423f9c94a90af2185d38cbe2940a459d8409d987d04a1f3e686c2b91d4fae1f3e3bdc5a30569838201b7d30c7320d7cbd787bfd6cd40e7e2d071a1":120:"fa31e58fa32d1208dd8a67fed44033":0

AES-GCM
NIST Validation (AES-128,128,1024,0,120) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"9c08d6efb167beb035f71554f64c12cd":"704f59d5202108b949170532ac1e78edb0e06fa323c1c69202d7d22dea4d7342199cebe949e980a21ff0fac282b868cc31ff4f6674c393c0f2cae2374664314afaf7791974b6bd6af26ade7fc266a6cd2de4f3c1f479f895ff597998cc8b929c1f05db13d9b9a4d98c9bc606eee32915bbdaeec6576e1fa6e8b22e0bb1098074":"608d56f6dea2fdf175eae189d42a85fb":"":"2c7d2618808adcf8edf5a54119471b930e07488d5fac3dcb53f4ade43674d162881bee1f27dea6d158b254d4b432e17f211515bf595a9874d89f8cf748ddaf2324078029c6463312ad32eb0aa5ebefc31c7fbfd04b37ba6b766375952c211d160b943e9d3c5e144b581157bff9071d31cfc082b55c4a0fced386ef2fc75e1a7b":120:"7a1ae03e2838294e286dca4fbbd9f1":0

AES-GCM
NIST Validation (AES-128,128,1024,0,112) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"192dbfdf86e48bf18710e706dc90e356":"1d7c45c8ef6f9f073c7f186e4c876c2b8fbf22feeecdc111a19071f276e838ab0572c9a68e9ad464fa88ba8d8a162e9f5ee1c4983395a890990357673467988c057eb8a0342c41867baab41456edc3932531d1c4aa0b42ce2b388d2be579dfe332f40a9b864c5e33e2b3cfd73b68d65c4db9ec46d3ba1587a56cb7887dcb3c5e":"1a511f85e0e138f4241882c20689f881":"":"3e50e821fbf83433155de7b4eb3c9a2c148b08d9d3998a3486f517fb5d0a1338faabbf95e85fa9186385bcb9e26aaa5e473d3cc7af869872e4fb36ad16c5468d994e9c71a09dd2868977f3f9064664f6ffcbac1bd313a7803c304273d69ad20369bad36adeb38480563bc6db9aa0d11a0e03d09731171c1229a756037b2c285c":112:"9393edf0934796eb97a8c513bbfc":0

AES-GCM NIST Validation (AES-128,128,1024,0,112) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"daf9455bad8bee905c6cd464677b803f":"af04226cc6eb84f8167a68c2cfde33a1521dcbe781e7b97a3fae732bcd8c0616a588200328902faa5a65a27e769a720d7ea23333cc1c66c4d

4e4c53facca5d6af06aea7fb49b12b04cd6ae38fe28d71cd66f769d640beeb07f508a0e3f856902cbfde6919077de378cf0
486cf177f897cd0a56b69db3a31b448ebbf8fdf63736":"6cfe8490e892f5ddba8bbd1cd522ba0b":"":"e5622ca7360272a
33e30f7fbeaa00956e8af0d871c433c070c8854d818eab9717293e845106770ec07da372c75266239a225ad74465e255
520218c6736e51070477d70976aa7d449c32a5c85bbd6931c76e9e4355f9697bad2ea3bcc0be005da15c62db219b074
b71fe4a5512157143df2c1f70bb17c6d3740d8d20eef88535f":112:"25fe6c9b2303b40ed31d1beea39a":0

AES-GCM
NIST Validation (AES-128,128,1024,0,112) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"82d166dddcbf4f7f66aa5ac6b12516bc":"7883f4f96c0ef7f6d
9fd7c2eaad25995943078559eb24a3e6650126ddaa32301b04f737dc27b648d6115ce08feac862cb888073b22aa648c7
52934bb7f9c566209a97499236f782758d6f6f9a012a2fb6885ca91858f9779cc93950baa731f1874629351e618693547
5a20593f66cddefff89be0fc0f9b57695b147d9acd8157":"540c2a07689bf314bc8ede71df3f4358":"":"44806e76a40bb
bc2de860cd36e93d64c9f4c11994f754db6a279d6eaecfdf19966512de5223d8332a407381114d50fadb03e33e347a5f4
d87c3fbf35f2d5967ba295003a2c6c12fba8394aa5b7a31365791c630734a6b2ef84eed0738cb4bc229e93c4e8529aaea
decff7ab93887b9fad5f05a88a5ba9fb449053ce4c6375d1f":112:"756d65c1b8a04485c3944e2a3cbc":0

AES-GCM
NIST Validation (AES-128,128,1024,0,104) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"81c1fca371968513a68ac09a7459042d":"182cb89c94171b6
85016bad76c445cc4561aff8e3170dd251f62efbd44910ddf8eba8a67dd1a237f2f7336f436edcfbdf9928e94c34881891
10d672488c6c4e0dc4a1fb6e67dee9a1bfc3f49d2f934f305f139e98f0ba9c1ab56b5ce9ddce4ab54b6970bf6499e5e825
abbb23f9e320ee05aaf0d712c09b0134839c5609e178a":"7c962a92b8daa294b4962cc3020dcd0b":"":"f91e36c79db67
89a3acec9e82ec777efc1958e7e5634d30a60239eb7cae1b48f40557965e8a6f6993db3f4ae443ba167753c89f52f610ab
69159ff60233310c1bb2baccb936433270f8839758bc85c53604e771e3ab0df6d6bb02e860d0eb27f425c7d30fb7566af
f982d289228da5ce5a45842e10ffbe9016c9e926d7f69863":104:"0114c2de8f733fc18f203150a0":0

AES-GCM
NIST Validation (AES-128,128,1024,0,104) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"09ce73e733e880c6d7be92be3144db40":"a283e20adb6efedc
5530f4efd71840d5fe61c902a7511cdaa939f5030880f3675959ee96e39abe082a66eba2a5a93214b22c249d7167b7a0f
da360d02df855d508c7ebae7016137e54290904909b2d41a59942abec76612b17ea76ffd1ee715aa2b05b1314c0ab286
31f3934d0e9efe2aef0c711e75a5c62701b3358a414958d":"f72a2fc910fdeeefe8743f57290e80af":"":"fe9a7f59abc372
0706c33fa40e106663d26c0f8da0d25deb90ada8130b6f95aaec07f4a7db342b678d102b2c81464e4ca9458732783cdc3
a9d504232f44e2878b0aaeec0f88efa5d7e5fb146911dcdb4569de7f114e1854ad7a95894561bd0fc4d9a5b58b5164872
833283ed88fdb4900b2a596db4e8379eed4e3a5c08d5fadf":104:"9de97bfec1325936bd171c996a":0

AES-GCM NIST Validation (AES-128,128,1024,0,104) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"e61d415db78d9f2695344350e0a8291e":"730c3fa9e07eea73
a734b17fcbc5a969dc2c04f448f44c7f6276e32ae3504e9b15fb664908f530e83a74e25a4525f74d315ab85d7b8500540
1370dc50fdb86e97baf3e7acb403e476193527a1a5d642ffad6cf2555d16d28cf4c4127189056389368b76aea806906b0
a38b808cb02378eea48edc005cf2c21e6547502e31d2cb":"e09dee93466a3f35605b647d16b48452":"":"ae87e754c1af
1175b474b0718e3560240f55194d946d101e7c0bc7af18d90a50fa41d68516e45dc2a4dba48d457ebff18a657a873e15
620ed7cf6ed3a26195b9d354ea279b24ec7802e4e95d3f3765188a64d7b8d4b7c215e7d67385efc6288724a33a1a7994
f21e0dc2970076af7cf31e9ad1098537543052a2b0f62e4e8a87":104:"5de3c5716735d7d1b859debb6e":0

AES-GCM
NIST Validation (AES-128,128,1024,0,96) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"19bf00b228ddb6e8f1fa4ba85f866475":"10742aeda590024b
ac2696af8402580d2ec6ba3f51cc6f79b6cfbb3057634ced6033fa43dbaec9af8ce7e9706ca699ede88d89caed89ea023d
14761bec49da724538b4f9672163a5bb5dbf92f5278fc0014eafce402cb408a1eaad6bc17ec0e835d6b80f4701f946661
757b9b2d54d1b137841519dd38d72835893ea6d52a27f":"760c5b929ac3d33bee4dae0088a894f9":"":"b03d27bc7f4c
9d48d555a38091347f371d0522ad4c347b4a23194c234c7877cd3621ce5a7c2fc26b38c7e6f1c2bf228ccec491f5bc352
556c08e4e19ddc4e4b2c036f45a42aa425a5ff9a2e9c9e5580b538ee56fa804a86d9b1b59b6fb0d00216a969367554629
79dc14990935919026fb51cdfef05b8dad03320a8112b7ada5":96:"2f1cc79408c85a9867214061":0

AES-GCM
NIST Validation (AES-128,128,1024,0,96) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"65bd9e7d9009dd6110dca657ccfe603e":"c1b539324a00190
1c2461b9747f605a2f4043b9b0f54d1357049fd1819de06df6e29880d62ef7d91f9cdd1108f3cce323f6c32cec16f7bd43
4e539fd00ada476ef41efe7c6907ad1cb726717ab56d6e2d32042ee2df3f90d15e1515f0a15a5f06703e06e14229d1832
8116148b3cc39683918e42927f62aec49ee9bcc19be38d":"3fddf7e943326e431be540c49bb917c6":"":"2813d6eef070
cbdee9d5d71caa8a88c631f0b71c41813c6219a765e4fb3e6eff9afe8f8f4394fbd5646fe80bab78806eddf7549d6ca3d0d
16d47ef63db93cb5620e3814efd86be151b338ee6e2c681bd37be4039b2ea4a190feccd7d65cbd56ebda81f4b66ce12cc
3e2cece731c37d4237a9dd0a2c1a7697bae42176a673d62a":96:"96200bd3e64d5eea746693ba":0

AES-GCM
NIST Validation (AES-128,128,1024,0,96) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"b9b8ac9215289aa003cecd53a90e0407":"8a6fbd067144b6d
50ea73a2a7abba3ee9677bbf00312c70d808fd124541ab936229d59842c8846569a063fecb8bd1945882abd987a93699
1d5cdbec087937f91c4f5513feffa1984a6b8d04a7b69eb4e93e90b6825778cd2ce9a0ce54d4a468c93884619f851d229
4be0bbbeef5fc0c05d2384126289283d5ddaaccd89711d73":"27d367f3f0c60acf921f8d8b228a0b2f":"":"42d98ecfb4f
707ec233c7f990b0cad8f39546b861b11d8cb9d939b29ff5ab315229d946ff55927dbde82c03aa73fd7857b2ad38fa55a
827dda54d2726bcee66347ce42c9cfd13ba1507d209ff2388c0ea2474e17e31d8056593b722d3c2a302a716a288592b0
a36547c7fd47f7595fee9d30f5bc09a9555d7f3169e26a924db1":96:"d66974c95917ae1bf79b6685":0

AES-GCM NIST Validation (AES-128,128,1024,0,64) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"ccbcc39512425bc32350587f0fc3e8fd":"57d6ccda317b7ea1
50b18d9558b39fd78d9cb52509aa5c095c5b46da89b79918c85d469ffac7226caddd670ac8f5add47fc382df1f32b4de9
cc1b2ca7c2acfbdcaa08429b97e77eedea55c8ddc7814fe4c3cc1e21f95d94301ab77b4df7572d0b8778cb2befc0f4c4a5
e93429ad52d6c2a75481f38d92edb1dac563154bf90b2":"0862ebfeb40ff24bfc65d3cc600f2897":"":"e6a77e90750cf0
e4c276c50c3880b3f6fa357179cbd84e22f5b43cd10abcbe04b43f191ed3fabf83eaca886f4a7f48490fb1fd92ebdacb68c
5158e9f81243f7cadc7a8ba39721df68dbf2406fcb5dab823202ceea7112e5d25952de1b922beda271e7677421fde25f8c
de450c40667387e5abf8da42dfe891c52bdd9f5060dba":64:"927d13cb90ee5f44":0

AES-GCM
NIST Validation (AES-128,128,1024,0,64) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"396b53a694b28b717c104111c4752074":"bbc3b818f4ff10b

6822ea41f63ca53c27578a8126f5163a5014c60e1bc8c1a9bba67a3808c8aeee09ba9e584a3584e9b86895a3f0db2e64e
71bb18b843b12f4ebbfaa1dff3734196f70c5a6d970277ab5337e8b940ae7c957646f8e96c6b5d84e9e97b620a926e655
850d09bc2d94678704aa45d1788e7c23ecf37e2904a0786":"0981a151c6f6867d3830c1f9ef99c433":"":"72a5587076a
1050b2b514f047ccdf7176c118db9236c0f72091513da39d7416734ac50e0a35b2905420214be8426a36e86863c99576
93292bfc5bfc2e93d234a09e80f517edb7cf8e5d21d5ae6c2362b779a9b62b4c66202894d369d219ef0e4b52a342b71f2
48c18ffc345dc7eb0b47b3bc83ffdef921eb42b6d51abd889ef4":64:"af99f8797495dd16":0

AES-GCM
NIST Validation (AES-128,128,1024,0,64) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"af090618cb454324a82a75a91944dd6f":"3ebca6ff138c527b
851b27b9e3917bb9a07282197868351dd599b74b332610bd634422911393171305caa4fe3f6e89ab6c033ca759e118c
2d8684b903966999125c748e04312ecd2c1ac3135c3be2df9c8c67be4d8303ac7aa6c21ca7b7c20b1108f5622d8e6079
f41e4be4abda99f782ad35a085b7db83482dc71b8e5d8e71c":"3380a6f20875b7d561c4a137519cccd3":"":"6be8eebe7
af78c062812513785e9803f302c771e8215e4c606fc5eddc3efd8b12c96e029b4287da55d8626583e58ce0e50c4ac5a39
a1b0f309d5803386738397376c0ae155087f36fd86fdda4b5c8dd079011fa9a134ca8a76de570ef165b20d7d803544cd2
f3a0ffede9b35ca1c982978bf95ac100af755553fdac38d988fe9":64:"3e869dcac087aa6c":0

AES-GCM
NIST Validation (AES-128,128,1024,0,32) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"041cae51d9e631ef70115be58f8818ef":"f6748f4a261d876e3
7fe44a419cfe965888aa5ee195ae12237322f6e7ac4bfaaf16e8e29be507e2978339a1855ab918485011fd52f834bf0876
ba8d89dfc01927e0930d03c0ac7dc7ba1554a879a2051011bcb34a5e4c7cea4d4fb5ed53b41ec8d17bd52b2e1b9dd417
a84ac5913ce3f9fb04daf4d14be65f49d0767b9431b47":"c32f227659e0566faa09eb72d99f89c2":"":"f30fe6c8765c8c
0af579c95bc2d182ccc346e587a57aa226eafb692675377a85e9ee08339a047b9cb674dabf5a25301d2c8c264bc06573e
36e55ceaee39239e367b8f1a3d781a2020e548001f9f98850994c3aa79b13dfc93c1d7291befd91e044b2f5d2583d1a9f
868fab4afecd46fec7d315b0cbf8a7331ef8f588d75f97e2":32:"5629e1a4":0

AES-GCM NIST Validation (AES-128,128,1024,0,32) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"f0577d9a7dbf7b4ada5b9758eec4c847":"5b5597386348259
21b5cb620b5b9f637f8b7ce33998cce1ed1a23ff01f84e58255d852a02e59e4394752405ecc15248f7616a33e64936f72
6de6fc6d10c3fce9ac0b3fcffbd755f16bff8462b3be24f7cf342c8d0bf1ca79b1cb4ea88d690644998a8ac3cafc8c18c8cb
737e38a681026d46966b89c7d6c7a4ce7a1e1faecdd5":"b432473ae67205bc7a99f5ab2a2721e6":"":"ddfe664e28c5fac
e3761deda1ab2dac6e36cfed538e3faf9d79c54e3c85b4baea9eedcef7f8f28c2feedec72ab2cc6aaae101b99512ef18e759
b7828364e4daf9a572f8c6ad88eb82f7304989345aa4985e498dfebc58cbc45aa31c18c0dda5b1991fd998901c65807c8
cff6058b1d5dfd583297da8451cef13f246547ad11df":32:"ce55ac00":0

AES-GCM
NIST Validation (AES-128,128,1024,0,32) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"6ca1d6ae9b5ddd6e3d68656c508df318":"d160740aed955e3
0c1f946088b5bc5bbaf5c84f282c32f65d099509993628ba5a51b411c6ebf57d58e9176b490ab90fa8db8a3cdc67a5f83
22d06d719d91f00ca07aa2a3977dd0838487f2e9d4dd285067a1f72bb8a6c9dfca107acf1f404995bb68ed9d7e12423ef
e570f144e0533fa34b8d0b7156112b85c94a8fa33d7a6d9":"68a494c9002dadf4f0303dd0ebd600c0":"":"276e362cb73
b405b10a98731333f6accf0d19cb96c21419d6d56b30dcf73f7208906b0e3eb103b721cdbb7eb1d4ff29ec3b7e9d43320
5bd9ec48c59d0075a1507ddf09275426c0ce9a58b973e06d6fceee7054ba92b1df771011ac73e39e451d9ac3375c5956

31090a2296d423e3ef806ac20770abf78ad04114f65661804fae":32:"8ff9a26e":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,128) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"5a3e577743b4581519b84b7538fb32e7":"172a0a14820448e5ffd017c18ee02219906f721c915c4f0ff13b7b7889812c0edb89f28be0c22deff76bc975d1ef8ef3fc40b10cce0d78933aa22e6adf2d4b7ee4ed6ef487eaddb666afd8671427f7525eb99af54a55d98159fc5d651266c65ccd915cbba60fb6e2c408ef177d682253c0b5410d77d08be1d8f175ca360becd0":"1e155ada52e250cee145d69b4a307bc0":"b9be2145b842d2f5c3d15ac032010400bffe31856441cb484d5c93e6710194b13e14077e132cfe03985d4b936bda9383c22c392968c748f7265213a8eac584aaa11eea35589e3536e39b3e4418248927fa9fcc027c5516e402445068ef793d349eb778b77fb0b37f51bfcc3c21df9999ca9985cc5bec6502445b068c2d061f41":"b5bd224140d6b826062e55754299a43a87cbe861360334897e82b7a6023ab0041736479c9aaca7c73f27e239a63e7433e048a8d2c2d26f0b18476aca7ac20837affacdffb57c618ce5982ba61fe1792c8a3a856970c095b0c4695dce961a354135075e0a786192d5875d16793a3ad0e3572a81efa24099f5ed9c92df55c15dd1":128:"74df58fd4a2a68657ce35a3ef11a9c0b":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,128) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"deb0ab6e8b0f392af6b89d253e923f1a":"14a86c431bde5c0861e6bd2cb748a13b9bfb2a4a67a0bcf067960b3a9c7a75fc7ea321863c83693c70076462ec3179f4d82ed4a1155a4b5004842fb47482bd6a83804a05af2504f6f535eb9bdc95a9a2eb80c7dcd7dff54e3c00437e4da9c433c88f6d248e4754656acdf8ea7d68106b04ebb2f1cdb247fddb0bca1f8e9ed6a5":"c1bc587c3440f1f5dea5b0a4b5ee8dfd":"602cfb09e8bf250c3a2c248c4e91234629a4fe9a18c5f8b59df215e97dd873a7c1204bd0695796908daa28b77353e0e5b37877a7441d35633119c0aee9aa82c3c18a7f577d09293fafce1895dafea42f97222a33b001907b978f11471cc0adc46243e8f7fce94803d4d0595bc9fccb9b9396b52deb943280eac2c4eda54841bc":"a72d27136d0b4efc0aa2126a246ae4946e2c62cf5055f7bde263e7516ace2b7e12179980f8dcff18dc4fcd662f38d3b9dc7f8a057827ebf27e5dab85264d9325e0eea3b12f8e9e39ad686263df75b0758cc8af0be89882bb159c95b8de392b3e295c039a520d2e56b50a6370afa57adc967f7e4ff670dab471a57fb6c81401eb":128:"eb26cdf879e0cb1320d786a642c4dfc0":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,128) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"adf6006fb1cfea0f9641a4c35b864101":"d21777e1fab632bffd82a58cb732794f112cd88bdda5a7a8d19c68ace343fd786e5e512013887105c21299f2d6ae23cae4f03047c68f019d98e76d2aa1b3a204f13f4cba13f5a8957b9aa3ebb44b8024b26cb6139a3bca3ada0520a68b8571ae89501b212a1f8ede5753d557ad2f38d9465dbb09b555300b13194bf7817321f7":"a349d97fc677d8ba6f72e8cc7191ab78":"5717bee8b31640f3999efda463d4b604c1cef62fc0dcc856efb4c50a8c6b902019c663279e1bf66fb52d82f8570b9a314647f4b1ed86eb89f4be8981225f94d4285f5ca9167434a1569b520b071ee4448d08cb8623b4cda6d1f7ad28e51a2df980b5a999025e9ba646707075a6cb2464c2a0d5fc804c98a79946fae0b4fa61fd":"345af0d804490586c9ffbada0404176f4cb1331fc77705175619f27d107512d3e6068323b276743284feb938c5718a5b013305fb42282a89e270d24585236fa18265dc7e8ddd2b3efe93a2ea05ab359323c75211f2133aa97022c9a937a467af37c92a795c682a30f2ba1c4ab2dc45e63c56cd3b29b0efac2caa3150e6a72aa3":128:"ae7d2827c4f1422b728a9fd31d8d1918":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,120) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"97c83d4628b65d94341984bbc266dc7a":"e998cc0b7677fa2

e504994e99cf7bbd84ba7e356d7da178f8ff40dddc046c70554ddec1d28aa23f9c4e6fcb9effeb8e28a883ad05bd0a6041
b8a24d0fceff200a4e33996e279cbf029b11d58185adeb5e5e797a74d0d8b17adcf06dfbe3ee11d8e6bc3b6a8434de6e0d
dfa0fd08c913f9fb911cefca72bc3f616b4ac9821f53c":"671dcc5001c2146bf8a4e522ad702bd8":"9eb12a42d2ca06a7d
a37fbc23d213f5e3f5e15580f01b0ea80eb4b6bd283e307dec965745ea3b3509d3269cf25808fc6a923e97d87d0c1a30b
447a5a27a06d0c88a96cd90d990bf208f1abc4934f6a0ae34a694750a74ffb27f4bb66bc799d43570b01897b98b00e6a0
1b95b356b11d33e852b2010da5785a691246d0be2bcfb":"5a6d8930e473e292e67425748e8618569b7a478f1e183ba4
e4a64385ac4b75d3d42b1afc34cc6daff341f10c1ad8f03d77179f52a7239ab3261f5fcd5a0b4282d26fa4d08bf0c8a5c96
782c073ad63ad233dfe3aa0290a03d73de14d445b9ce4ea0e3b10a4aef71c5919969b7086353c942c479a1c052a749afd
e2325ef46f7f":120:"b81cb7bfd0aaf22b7233bcfe363b95":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,120) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"2dcd5c974c5d78cde0d3a677d0b1acdc":"21b61035ca3c149
d66608d77edd9770411e0ef73a97d4be9dcde95ed7997ba97117ae6c1979195a5d916ff7a1d43ddced5287004fb60a2c
81c82b5f7c8a336a603c3eb7cb160bbf21b454f810681450d65deb64e7cd229333fc5e85dc29040d7da48511b6b2524f
02eaeab422b5ca817796c47b9f2d7d498abc619b2ce2912bf":"7455fea1bbbfe9479830d403e33c9d1c":"d684d38f2b1
2111197ca512c54c8e29ef1c3b9b089a6923cdb327c763f0ac8c2ec0900c716e211e7cba1d7c13a60fe87f5d78e5d5215
d92e57a0645d9b2eab4b11870b5f7bfa9f2c9e4b9fcf7596e7719b7d0c0e6cc16efe71d8bc92e16a83d4782f08e9b97dc8
5a18c435b51c940189a3c2608379a21a8c46633020b9b6cd10":"eb039d8cf0bf217e3f2aa529ba872c385f2770ede6ca
4ed32fd22cd3fcbfddfb92d681f00df6fbf170a5dad71c9988d556cd74bc99e18a68683e0ea7b6ef90b21ff42cef8c4627e
4051bff0da00054390e10036f430dbe217e5bd939295d9c9f64c2614d42ba62efe78763cc427027edbd0b7f72eceaa8b4
776ba633f2c3d500":120:"18e7b50fcec11c98fe5438a40a4164":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,120) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"e5b132bb7aca3e01105848f9b37ff516":"3b6d1a432b7fdb40
22fc35d6b79ea03b6aa14d4ddf60a160e976909ca069242fb2e7d414d4e34ffdf9416823c4b3f4e018ac8ca689446647e
da6a12029f886bcc9d18be150b451d78fa72b9c4dc13314077a5b04cffeb167005c7e8379940e6b998316bef9bf8b5a74
2e337663c0ed91d88d09d0c3ebec37aecaeb8277b13661":"24c1ba77d37f99253576f4963779fd59":"dedf78f05957bd
e906639bd35eacd8fba8582d288c9f14a25eb851a0a34c82fd91f2b78614ff46ca17fe7781d155cc30f3a62764b0614d57
c89fddfdd46af4fa5fc540b9ee9076805d4d121aa0dad2449d228f1fc3c07d466c051c06db6846b9012e8d268c6e1e336
121d272ca70d965389a5382fbfec0a439e979f16fab0283":"9976d2f3e16485b6b3699a541b6df386562b5ea4f6f9ff41d
265b16e2d7d3c5f131bb5874cdffa87e704ae3cc24f1dccb62babab dcdedf8bac277a7277ca53a4d38fd31f9fc83f86a105
663f045b70dabd553137b6d6222abb334b7be7689a4afa28103619f11b8b61aa92a63136ad5639f11bae64b25f09f1e2d
b701938fa5e":120:"29d1b8a68472f2da27aa84be714108":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,112) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"63628519a0f010620cbae37f8ad34570":"6db2919208b09a8
abe5e95dcfe0f957dce1ae0e5b29f06bf321dc815ceca094f38c5c812f591aedbc9fc28cc0317bd1d89d4a3ba14f7b3e5fb
2e03778990a6006e0ec2ceb47c923f3b17473f99521491a4cb2f9bd435e3133dc90e129ded9d15d78e75bfb3492458ce
0964d5614508ef2a38ea02ec8664ba901891a7cc86a62b":"ce0ad75b94ab2d3918abf255c854ecf6":"c29384bd7cd013
fa02487867595d739d99886a3bbed7fd5acd689f3a74f240f14c8fffd0bdea1f83bfef7b58ce512849e3a986f37afa54ddc
11719169a49bd7e7138a745053417ff80cab1a32ae9be476ccb61ae055b319fdee5dcab629bb237aeb7d998ce36dd9c69
08451c3bca9d3582f7fd60e69f6298d43a3b958341b611":"6205d37d720cbb628dbd5069f38ded8e566030eadb7fbdf2

ed827d5f5a0117a21c75ade89782b3dc4e7307d9a7ae406ead0145aea1b6cce286103a55ce195999214b84bc25281bd7fe511868a69944d483e05ea6b39b11558ab46a33d227734eb3a386e30d58c3029ef0cb4046c0856078d57a6df194aa8c0e10f9b6ed8fb40b":112:"423fd542498825cc54501cb42b2c":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,112) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"7c0e1c6bde79315f79f22ebc77107228":"9cd56b16aa4e130c3dbf30e701e8784ff39f866031e778e9ab72b858c3e333e9589b4b6cd89d6546e52a478d92bd59d0e4756d6b5037ab1873d88242ef31be643745d26395385b71034f6f0c0c84816f0c6755965fc8a7718f891d618f226684bcc77f87fe168e178b330d4b4c0eb4791028017fe6c42e68b0e195654a5d65e5":"9011dee57c3b8e112efa4d2b816cf189":"57bfcccc6f00c0abbc5f30589dbb47597838fdd50dd622eeedee33824e63ba78753c05d2543687f60dde501757b6fb74c17fe34b3e9c455eb38cf078c8c77eff68d3e3b8c244cde70ddf61703664d34159a11785cc6626eb1cad70ab94405616fff52c0f781ee6b43ef2a449924a76b762035ff479cd6006c21a62a56a14650f":"2c1ef998747163104e5a7d2a440a1a1cc2c20446a9d0cf5f138f85c1f5afd90fdc3fa4932845c150518f40bfd56569a5479126c49061ef350b4fae895170b4eb94dad7b456890a822e1bcb57f9bde5bea747d17be3d18ea201cd99bc46fee21132c6918ffb0117744f6ba3f25bc8a50f9719854314b934c3a3230f4757a49113":112:"4ef9aebb721dabe2d09101037a63":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,112) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"93f3fa85dbdb2784fb078a34b1116eb1":"e7a0fafda0b90cada671f5e2adfd2e2a5f14e4613ea76aad57e79e2cb532f655210614e2036d7ac005ed5e516814d8667ed71e0f29b9c7b470f4722327407cd6ce6dbd298cee37bff33c35e34cdfebbbf33934673469d6b98becd6d26868977e69e06deee99c118fd4da3530d367d20d15107c03efe0d7e7b38710231e0dcdf0":"f5a7b0b26d1e86f4fc69f81c9eeff2cd":"3d2a1dadccc597b5e7b6ce48760150dee01c8550b525c587abcce8c2c7fb6291683a58c2e42e7b7ba6a3c2a117ddb7e67ea058a78989d67946fd9551e30fcb52618dcb9fae079ca56b74572d7b6a7b6a5c60e906e9639eac5ee1a5a2db864721119da2c4c5110c2b8d487e792cf6929600f1587cb2d48efe6864019afc32af6e":"60da3f4b3a263bc0178379646bce391bf552f60d2833261962375d2960c629dedac681d86f7915ea3cffdad0f37e409668f923d7c860525b994b325396531994a2fbb2d4e909d0b1dce322e078b4b8cd99820a39ffd7b468bd3e73b418b9a2cd5757b7d45f0363574c925bc22d66645abd95a6b29ea6366d8c2252d1c5710d45":112:"833d2c55f5ee493060540d6b5349":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,104) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"163c05f69cdc4e518ff6445911d1ede0":"84d8a1855423293de37ebfd9715a9b46b175bc6d44e94ac8a3e7d409e8a227a57a6b85144a8ee23564fadc28742b69e89c0d4aadf0a786f9a5d5f9198923643ffc0bfd0f96e43b08f1435d4afc0e49c0e2241d938780975bc7a31cdf38f30380753bdd66be72b4dff260a35dc10b9ba35059ba61b0beab16e35068721bd950e3":"4b16188249096682b88aa5e4a13f62c1":"a238d1111efb7811f6838c3cb6f3bf3e0ecee6d8efb26845391f8adb51e497e840ea40318bf8e3cf0681c3b69951c4f03d5a4b5edf7119a150eafe6dc16b68f3d2b91e1454637135148f4fec132bfd96ca088169a35961d4c663535b9852f12a00ec4c08082553a09ea046379ce747c717036154d063d876a2b95cd7bdb42daa":"3bf751cf63bc1b433be6075303986ac1d0592dee400774d0bb7a9e72224417639e1e83e69f34226b873365f41fdac925628f32ed4b572b374310edfd892c5e0c3197e59efbc22ee11f0d4a66bd73a6f5b0de7c1cbb0612a63a262af51d418577a9bae0a8577e547382878f13047a92f51a867f8b7d283d2099c34c236918f718":104:"0d778299c4dc0415ca789dd5b2":0

AES-GCM

NIST Validation (AES-128,128,1024,1024,104) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"a2ff7cb9fe33b04a087d9ee6db58ec0e":"ed7c22218009ceb5b322045fecc1fd748f27655397a09c2c29813eba9a5cbeebe88d4a35dfd741ef0ac1d11c4adbc6bfae824af88e3ce09f68d8ca7671de91ec9e2bd5f790d1cb1748e34b3560c9b10726ea4b85b127731d8a7fdfd0ddbed11aaf181799f71a68e542b43ed9889237d2fffe370f41064b810c2e14d1ab661517":"6c58eb8f1f561b180f07ede0d3ae3358":"00cb63fa0cf526c6db37e33cf092f3f421fd258d28446c9a7c687b941c7eb5e1c5be267db992d0d93ede0b09030f979d451ecbdbbbb386cf1d74b23d55b74f5f4d520c000c9a41922f54567ca7dfcd84c68883a23c7acc3db3cd8d340217ee7c5ea39b41cf2c0e58c270a19ee9e146d2dbfdaf8ba3e24fda7f2c5e4ba6563ef4":"f0f119bddf5ddf147fe06da9d4510d97369d8e345519df2188b8d2dbaf8b7d3e01f3c26475141aae224e5ce1b131c8096f0e2a17c4c2df62f76f009cfc8aa20ddcd75a6a4281cfa2225485ca22aabcb60ff11265acb92a19ed66797fc2b418ae4b8c70fbecf0fd63f6c22ad62bfd6f40d8d0e2abeb620b7b4f5d8b3e041a53e6":104:"7885ca22c4afd7dc6cb440ea35":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,104) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"2e739a485b6293b43535379e3b309fe8":"699b9a5668042c48c63ffb323c0fab18446546417b2f33a69addce6178f9d5b7dfa891ff2004eb57a98ca012c2668e0614276d89b21b7bfa436b2aa1582daaa81a6a7722186e99dd16a5786fd0e8b09b194746232fd413984484524793a379112e297d733dce063408fe59367f5929c5086bc2191a8fdd60a346052c0d109d57":"c4deca3eeea80352624c93523f35e0ae":"704aa36a82d02c56f4992469bb7e8a3f7dda1326068bf6017e4a0c810352b476aea129c1ba1d4974bc0d0503dcf816b89c0dc8e6d066774ce97cea65b5fb5c7b5a7f93e5e2c7126dd3b241b958e47d8150b422bb91c4afc47d53cfc2d20176c2ea0c85b376dc46a86bbaa53c584aa561f6662d11de4e39e50f1a095b8555137b":"30b8fa2e52577a7e5cdc12a7c619615b134ad4b41893ba9120651cd35c6f2d48ec6b8b9fa99366c4d60e643a8ccb2cbb3568f7647f4ad1a12d14deb8aac00dc4ef780133ee8df8f494675deb7f678fed54e70d6bf43476854eb0286a49cd322cc18daa238d4580ee665fbc759295a3e12567beff3e823811093cf0f02d00820b":104:"ff89ee52fa4eaeb748c8676490":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,96) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"6bbb12361c95953a8d757bcbb92568eb":"c3fccc5693abe53a13e5209f80611fad1e81e7ce19a4612666d954b4b6d2062bee764181716d5fe0fe1de485bb739d6e8625d5b6cedcaaf6e4e5ec350bc2168c24d7764e75b0cf079d7ad1b5fc24dbed14c5ae4714734f424b3611de0f70a0a8d752fb143e1b7e51ebc965a06021de3718af30b067dde270d804fb5b87ffb29f":"48ca821e5e43fd58668380491d58cdfb":"e97280fd78eb8bd695227fc79420971081de8f24bc95d9a1794ed2bebf5b68d8b43ae8288eb5ce72db0740334ff9bc9b4e660418d3cff8c344e50c7962c367c26247806d0b5c2ae0420a724203dcf4fdefd6513f8263d995afa4780a9c4e92c25496106fec370d0450d907225190ecccfae634f11f8f74f6422a652b2b9af9e5":"61cfc5a6ab6847bf0127b35ce0712cbfa9cd28dfb3f0b4cac2624c52cf55f311e55e9abff2d4514c6feff801ea8739f874ded2efce4a440f2acd95eba6c75e09bcd91b898c98563a26b3df415658c4d04a6aaf547a90b03d1789bdf7ab8f09f6d9f222f567461380372a976240b7b180c3fa7b4507e53815af3f6b4a46973806":96:"f86d5374d1ad269cc3f36756":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,96) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"1a0a9b2dd1ae31b3e47b6df979dd2fbf":"353786f96620ae7dfa7aee163c7bb30384bb324b516cad13872f48e7251f6f4c5906748bf2a2f6167bc14453b2b2f513804308ba92d69639beac2f25274bd5477744281b7ef7d0661b3672cd45abd5bd30d98deac4ad0a565308c0224dff59e3190c86df6a5c52055f8e0f73fa024f99162219837c999a9c0a12c806f01227af":"b39c8615fa062412fd9b6ac3a7e626f6":"dea75b17cd13dd3

3b5016de549c44fa9c88baf424ac80c4835e868acb58082ffc4255c655878a1c627a44160d5e5054a0a04f65fdfb542cd3
42be2aa2e000117bf8cd67b02f3a3700755508f9af8379c226aded404117a5ca3fa70968495eab287064ee584b4ce5966
12f2c465d997518c6995518e3bb881967ab6b99d7f62d7":"8430b8735f0b002e098d513eec7b3a8431a3fdac2b7faf25
6a7bcf08f3dcd6fa549f029240acae4dbd4ad54752ba358c14893aaa67a003261c252020d14b521906b23c37dd80af703
c2964ce13773dd72fa56c389768c6efbd485953900b56f6bbaa837f1668f478677621a297d4b5a2c1a86f689d8644caec
51435b0dd66c77":96:"f000f2d398df18534428f382":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,96) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"4da736fba2b7202ea2ba60793da3344d":"4f004852edd5dcde
13507252ed8c2b20a093ac9081ce2a8133c48d2807e5f968c04a20dd52c070d6c43c704b8650da7f94e5450e0d34cfc2
b2d2ba7cb5343e6b4281633c6c065dae27fab18ca71bea018eba94d20e78c5e3223c70f50cb77399c1a89436f1e721367
3ae825d4fc5523645031696df10f9b5238c03f733b4dfcf":"8572af442c9af9652a192d893c18b8c3":"429915c3309fba
2a42b8e89f42a9376a2f329805a4d6daae11e9a20c2f982671ef8a7539a9657777d03cbf755ef93be0d8e426ed00899a5
9e8b963fd44269d64692ed07b231cde93e85397cf125a75032ca3726ea1ff1b05d79f2040c1135012b90597186c1db2e
16cd128d45a7b9d934ec01341d9030e9721c62f62003059b8":"ff4e46c4236304b8d52ba2d6db269f95d2cd5fe4318ce
930d407051469c7e36e44bbcc909c4966276f5a2ec70021982fecbeae34df235a3e9e0370afa5a269ca8847a84b8477f7
ddd6055d0f800ff4d413f63db517c96d15dbe78655748edd820f2ee79df5eca31711870022f1f5394b84f05bfef97f99cb
d6205f8e522b3d5e":96:"624b0b5b6374c5153835b8e5":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,64) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"5bcc874114b9d78c3eb748a783d1448c":"7d57418bcea0072
47f5e18c17a2e4601c3eb8c89f61ed365d5aebee7593cdd63871d964a25fc9d723f291d39e0c4f75012471faf8e06db60c
4ad8a26cf434bd82a29a8b653fdda1b86a7e4800c1d70cb5d8b8a1d1af52894082bb282ffdde8f0128a4abb68aedcfcb59
160f6b5aaf452812f4d00472d2862a8b22480e71231b3":"5f4fde440faa9537d62e62994ab20fb5":"b5dfe0d971f2920b
a4c029d4c346a49788b499faacdb18b8f905f1457a8b9fa48709893516a7b48bc601710bfd73c12da094c29df5776d491
c9978f8ab237f605785b0304488f1c20bf5a767ba6d5e1e2961957aa107bdba2358b81ef1e06576db985b3ef8194725b7
5d49de1de3a57f161dede508e37ad3356134fa0a1aa48e":"6bc0dec98bece6c4e245fe978f6db113deca75e1b475bc31f
1da0c7457a85ee7aac8be5f2121c0610b99a2c64519fc2514b643c379b4f53c5432b9729aea9fcecb88a2e2d0a6e74be0
4859a66f55fb2af1598bcb039108ef7fcfd99d94e79287ec1f62bd1bf5ff9dd51ab12fae4f6e21b95ca50032f9a65bd85f9a
1aa0524950":64:"354fb8bcd38f2a26":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,64) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"427c89146eb7d76578dc173bd9e15cda":"1d39249130404d6
0ed40241cf3354458e06f1474b3723569d88235f03098053fc99010f39435620acc710a4e386b2ecbf9b327a8dcfbeddc
084353fff029d24787ce81e74a5e1ac1ef096e0a2ae882a669ca168275806bb7f462e66c941fffc6ed44b9628450e03a50
32676c1ee4aedfcb1767150d56c7d73a8a47f6d19854fa":"0092e76cd8882e5f77f4c8514491705d":"0ac4631358bb93
75e07756692bde59d27012e921f054fdfea0ddb242c43421f4c7241cb210cb5c172d053de2763efd565f1138fbe7f9cd9
98d825ab800df900843474ebf857b3371c555b89670e86354fe430f715ebbd0ecad974fea34e3bbae43d3ca3ca178f336
1f0a11fd75f60e9140f44364b02a073dcce8339fa28cb5ad":"2b385e9df4ed41cdca53a4ac8cb3e0af75eddd518b672738
0712950d96c34bc6a0a6ac02184c1987548932b116ec9ae7abf01157a50e422b3e6aa62deb0cb2d81bf7fe0c25041a355
ccaaeb049abb0393acfe90d869e9edfdfb646971bbb1ba9e5983cd0e2739158fab31be26cfdf9286d347b58b00f75d9f48
ece1353308a91":64:"905cdf228a68bebb":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,64) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"2e09660909a9aa0a50958016c3e07895":"d7b2ceb182d4a8ed57572c4237ba99bbdd589093db0f71732f9e67559d3054fa1af195aa4864fde413549d27468ffe7c5c23e242cab4ae4bb9e2657422dc3fc78fbdcde892ed202be1e47f095b09cfc53cfe86cb16e2e95444492ad5d0eef053178d6b0485731be7a5193563bf56f63cc0687fc01679254d74e9ed788645004c":"c4f865be8b5062e488b1725749a87945":"26f50acdefde4d585fc6de6c6234c9ead40684349a2bfd022df93d9774c9f5b8f50474032a417bdcc21a74da72c0297437a0cef8f527c9205797f77b4227c272e08ad0b120a2a31ef13e372cad2387ccc1bcefc88dd58899821d68f3be6a4b2cd08697d1897efcd6ed3a0d7849f6cbb50e46800627cfd26964e2cfe9f36624d9":"321f6d79a6658c7c2b67fe3c932237593a6ec7e6fd8198abc6b0b6ba5d4dac9e0695f0c64dde1c94c0383839ee37f8bbfcc516f24871fd79a9b9135ceef841e4c8ddf6b57962c0e8ad7aaf210e97a43489097270756404fddde637de461b8644fef244142820e1af12b90f16748b0915a6b773dfbbdf6b16f1beaccb4cd5edba":64:"b294db7ed69912dc":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,32) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"5e45d57981f65a6b170efa758cf4553d":"bc8d4c418442743f2fdbaf95b8f87b7c15a3176085e34addf4cf0fb3c2df15587526691b07e6407ba16999b72382635a2aebb62d05c1547a7d074c857a23107c7577864e7f7bcdb5b6d1fb50136391f89c42d3f02754b0e4ed0fcb0c03576b986af5c12cf9bf5e0c585d6aaf49d0c6fb2ec30eae97b2b850a35474bfb9a2c069":"b43403b627fe9e0135192d1a048c6faa":"7a27ea26c7607e4e7e627f3161bdf15f21f3d62dc33df14951971712f960d3b2082d75395c5008e5ea00d282d350f86dac8c61f5c0f90e7797a5b61ee96f7e332ec5de51cb1377e47c641f326d1e58817c8c95feb5b2923758e33b279191d0a9ffd09b7619b0318a70775e36abf5f7ab59422ff68914e7b478c448a7b141c4bf":"90d8a6218da063c38e0f06d548a3d5685fd3e0fbaf609c77bdd573bb9c63f30590eaf8b181a2feb81c8b3f5f34a94dc94b905036a6c69b97263302b8674d9e09325065588e97c0b5b33116981f1f362a7c5bb1e996c126c31fbd63791772f4d594632f408fdf011b3f2cc750b060452c181e8e09697c8662c00c8d4f29d875a7":32:"611abef7":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,32) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"00d4bf20509a61bc76430ffa5f013589":"036a191a388cf3c57c9e6f0e2f5c8bc3d5c25ee8e2fedfadb7b7433155c7e79304f0905ab2a17e1f04f2f2dacd4a41521d6ce213961df9dc9101d41df4e44246488fbedb75a01256fbc7784769eb8f99d44d5eabf93cf667ebae2437ccedc79efa58c075183d46a5c20bf4c81e0f9754ad35af65f7c8aafe7daa3460c6892b1a":"25b1026a009470a5ca8caeeb67200792":"fd75acfd5aa25fb8bccb53672e5d6a8080081506cf03df2bab0746a353510996e0237d6354ee0210a41f20f88ec6569f2b200b28c6a31464a0533a6bc45afef3ae381425a3606de2866dba694124d96da9d0a2b061b787524ee6e5d3b1ef5c4bcf168810aa177660b7e1379ac8a480ce43d73dfcc696873cea2df419f372651e":"cab80615b666c47fcabf0d9805842ab2805150abad4de0ae8b12306bed504d4a7f91f52379df65cb9587577e59dafcd4203d2ed2743d35472285e9522db0ce3dd027a01c79ac64caee29ef3752a077254b0dca269f6f206f6cc575e8fedb0ba525dcf6252fa6f7b688556933f1dee84b2ad36a266695ce8672229cedd82f20a1":32:"3287478c":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,32) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"fe481476fce76efcfc78ed144b0756f1":"246e1f2babab8da98b17cc928bd49504d7d87ea2cc174f9ffb7dbafe5969ff824a0bcb52f35441d22f3edcd10fab0ec04c0bde5abd3624ca25c

bb4541b5d62a3deb52c00b75d68aaf0504d51f95b8dcbebdd8433f4966c584ac7f8c19407ca927a79fa4ead2688c4a7ba
afb4c31ef83c05e8848ec2b4f657aab84c109c91c277":"1a2c18c6bf13b3b2785610c71ccd98ca":"b0ab3cb5256575774
b8242b89badfbe0dfdfd04f5dd75a8e5f218b28d3f6bc085a013defa5f5b15dfb46132db58ed7a9ddb812d28ee2f962796
ad988561a381c02d1cf37dca5fd33e081d61cc7b3ab0b477947524a4ca4cb48c36f48b302c440be6f5777518a60585a8a
16cea510dbfc5580b0daac49a2b1242ff55e91a8eae8":"5587620bbb77f70afdf3cdb7ae390edd0473286d86d3f862ad7
0902d90ff1d315947c959f016257a8fe1f52cc22a54f21de8cb60b74808ac7b22ea7a15945371e18b77c9571aad631aa0
80c60c1e472019fa85625fc80ed32a51d05e397a8987c8fece197a566689d24d05361b6f3a75616c89db6123bf5902960
b21a18bc03a":32:"bd4265a8":0

AES-GCM
Bad IV (AES-128,128,0,0,32) #0
depends_on:MBEDTLS_AES_C
gcm_bad_parameters:MBEDTLS_CIPHER_ID_AES:MBEDTLS_GCM_ENCRYPT:"d0194b6ee68f0ed8adc4b22e
d15dbf14":"":"":"":32:MBEDTLS_ERR_GCM_BAD_INPUT

AES-GCM Selftest
depends_on:MBEDTLS_AES_C
gcm_selftest:

Recommended key length: 256 bits

generator:
80:0a:bf:e7:dc:66:7a:a1:7b:cd:7c:04:61:4b:c2:
21:a6:54:82:cc:c0:4b:60:46:02:b0:e1:31:90:8a:
93:8e:a1:1b:48:dc:51:5d:ab:7a:bc:bb:1e:0c:7f:
d6:65:11:ed:c0:d8:65:51:b7:63:24:96:e0:3d:f9:
43:57:e1:c4:ea:07:a7:ce:1e:38:1a:2f:ca:fd:ff:
5f:5b:f0:0d:f8:28:80:60:20:e8:75:c0:09:26:e4:
d0:11:f8:84:77:a1:b0:19:27:d7:38:13:ca:d4:84:
7c:63:96:b9:24:46:21:be:2b:00:b6:3c:65:92:53:
31:84:13:44:3c:d2:44:21:5c:d7:fd:4c:be:79:6e:
82:c6:cf:70:f8:9c:c0:c5:28:fb:8e:34:48:09:b3:
18:76:e7:ef:73:9d:51:60:d0:95:c9:68:41:88:b0:
c8:75:5c:7a:46:8d:47:f5:6d:6d:b9:ea:01:29:24:
ec:b0:55:6f:b7:13:12:a8:d7:c9:3b:b2:89:8e:a0:
8e:e5:4e:eb:59:45:48:28:5f:06:a9:73:cb:be:2a:
0c:b0:2e:90:f3:23:fe:04:55:21:f3:4c:68:35:4a:
6d:3e:95:db:ff:f1:eb:64:69:2e:dc:0a:44:f3:d3:
e4:08:d0:e4:79:a5:41:e7:79:a6:05:42:59:e2:d8:
54:

prime:
b3:12:6a:ea:f4:71:53:c7:d6:7f:40:30:30:b2:92:
b5:bd:5a:6c:9e:ae:1c:13:7a:f3:40:87:fc:e2:a3:
6a:57:8d:70:c5:c5:60:ad:2b:db:92:4c:4a:4d:be:
e2:0a:16:71:be:71:03:ce:87:de:fa:76:90:89:36:
80:3d:be:ca:60:c3:3e:12:89:c1:a0:3a:c2:c6:c4:
e4:94:05:e5:90:2f:a0:59:6a:1c:ba:a8:95:cc:40:

2d:52:13:ed:4a:5f:1f:5b:a8:b5:e1:ed:3d:a9:51:
a4:c4:75:af:eb:0c:a6:60:b7:36:8c:38:c8:e8:09:
f3:82:d9:6a:e1:9e:60:dc:98:4e:61:cb:42:b5:df:
d7:23:32:2a:cf:32:7f:9e:41:3c:da:64:00:c1:5c:
5b:2e:a1:fa:34:40:5d:83:98:2f:ba:40:e6:d8:52:
da:3d:91:01:9b:f2:35:11:31:42:54:dc:21:1a:90:
83:3e:5b:17:98:ee:52:a7:81:98:c5:55:64:47:29:
ad:92:f0:60:36:7c:74:de:d3:77:04:ad:fc:27:3a:
4a:33:fe:c8:21:bd:2e:bd:3b:c0:51:73:0e:97:a4:
dd:14:d2:b7:66:06:25:92:f5:ee:c0:9d:16:bb:50:
ef:eb:f2:cc:00:dd:3e:0e:34:18:e6:0e:c8:48:70:
f7:

-----BEGIN
DH PARAMETERS-----
MIICDgKCAQEAsxJq6vRxU8fWf0AwMLKStb1abJ6uHBN680CH/OKjaleNcMXFYK0r
25JMSk2+4goWcb5xA86H3vp2kIk2gD2+ymDDPhKJwaA6wsbE5JQF5ZAvoFlqHLqo
lcxALVIT7UpfH1uoteHtPalRpMR1r+sMpmC3Now4yOgJ84LZauGeYNyYTmHLQrXf
1yMyKs8yf55BPNpkAMFcWy6h+jRAXYOYL7pA5thS2j2RAZvyNRExQlTcIRqQgz5b
F5juUqeBmMVVZEcprZLwYDZ8dN7TdwSt/Cc6SjP+yCG9Lr07wFFzDpek3RTSt2YG
JZL17sCdFrtQ7+vyzADdPg40GOYOyEhw9wKCAQEAgAq/59xmeqF7zXwEYUvCIaZU
gszAS2BGArDhMZCKk46hG0jcUV2rery7Hgx/1mUR7cDYZVG3YySW4D35Q1fhxOoH
p84eOBovyv3/X1vwDfgogGAg6HXACSbk0BH4hHehsBkn1zgTytSEfGOWuSRGIb4r
ALY8ZZJTMYQTRDzSRCFc1/1MvnlugsbPcPicwMUo+440SAmzGHbn73OdUWDQlclo
QYiwyHVcekaNR/VtbbnqASkk7LBVb7cTEqjXyTuyiY6gjuVO61lFSChfBqlzy74q
DLAukPMj/gRVIfNMaDVKbT6V2//x62RpLtwKRPPT5AjQ5HmlQed5pgVCWeLYVAIC
AQA=
-----END
DH PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIEnJqMGMS4hWOMQxzx3xyZQTFgm1gNT9Q6DKsX2y8T7uoAoGCCqGSM49
AwEHoUQDQgAEd3Jlb4FLOZJ51eHxeB+sbwmaPFyhsONTUYNLCLZeC1clkM2vj3aT
YbzzSs/BHl4HToQmvd4Evm5lOUVElhfeRQ==
-----END EC PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDzTCCArUCCQC97UTH0j7CpDANBgkqhkiG9w0BAQUFADCBhzELMAkGA1UEBhMC
WFgxCzAJBgNVBAgTAlhYMQswCQYDVQQHEwJYWDELMAkGA1UEChMCWFgxCzAJBgNV
BAsTAlhYMScwJQYJKoZIhvcNAQkBFhhhZG1pbkBpZGVudGl0eS1jaGVjay5vcmcx
GzAZBgNVBAMTEmlkZW50aXR5LWNoZWNrLm9yZzAeFw0xMzA3MDQxNjE3MDJaFw0x
NDA3MDQxNjE3MDJaMIGHMQswCQYDVQQGEwJYWDELMAkGA1UECBMCWFgxCzAJBgNV
BAcTAlhYMQswCQYDVQQKEwJYWDELMAkGA1UECxMCWFgxJzAlBgkqhkiG9w0BCQEW
GGFkbWluQGlkZW50aXR5LWNoZWNrLm9yZzEbMBkGA1UEAxMSaWRlbnRpdHktY2hl
Y2sub3JnMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1v8FswMughO8
mwkHWAf+XRpK33kYR0ifBnObvk2R9ZTEUk/TfFEEFVlen5xhiE0g8lbCj8Y5Mzsg
wZsJv5in/KnraYb7VC0ah0jx4sMkhKRcyUWfjyH8r7FNH1j1jd08ZpWJGotYxxaL
evqom1rzLN99JPObwyCCgGcQjlRV7cMfIgwlwHb/JPXOy/hYAgjrCjqvBu3nL5/b
HF0PyVGiKCEQiHhMBKNjAxzQrCUGy7Vp+3QlIYrs6/m5A96vohX/j+wzwIp3QgiK

Yhj5E4Zo/iQLf6Rwl7pL4RTdT+crcy143mYiShNY+ayl9snfVJNnuHaMe15fVEsP
X9lDvdBvXwIDAQABoz8wPTA7BgNVHREENDAyghJpZGVudGl0eS1jaGVjay5vcmeC
Fnd3dy5pZGVudGl0eS1jaGVjay5vcmeHBCU7/jAwDQYJKoZIhvcNAQEFBQADggEB
AAXUXoWlQxKvSCVWhes8x03MCude0nDqDFH1DPGIKeVeWOw87nVni+hIvy8II6hj
5ZfGSHuZci2AgElA3tXk2qDcZ/uBXe2VV4IwsgXKUYSlpz1xoU55InT4e7KdssEP
HOyrU03Dzm8Jk0PhgEJpV48tkWYoJvZvOiwG0e43UPDv9xp8C8EbvJmmuWkUWnNW
o0yDnoAOxGfUGSUQ1guTpWCoQEKj3DS4v4lI0kNmJm+oRE2vv1XealWEHSuMpRZO
Qhy8WImX3muw99MP579tY44D5Z7p3kpiC1bwV3tzkHdf5mkrAbFJIfliPvjMrPMw
2eyXXijDsebpT0w3ruMxjHg=
-----END
CERTIFICATE-----

```
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
   <Configuration>Release</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\x509\req_app.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">

  <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid>{486B1375-5CFA-C2D2-DD89-C9F497BADCB3}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>req_app</RootNamespace>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
```

```
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
/>
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
```

```
  <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
     <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
```

```
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
  </Link>
 </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
```

```
 </ItemDefinitionGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.targets"
 />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
-----BEGIN EC PARAMETERS-----
BggqhkjOPQMBBw==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIEi1oKInPLbiINj8OxdActVTgI+YQVSefdQfCu1ihbLRoAoGCCqGSM49
AwEHoUQDQgAEjTo+HeDBAO6f95ooo6huE6BOKKSjwJvtwUyBqyU2E9ePvk0olCAp
dAEl4/sXlHCzCGl0zdONrC7B8aUoc0Gi9A==
-----END EC PRIVATE KEY-----
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
   <Configuration>Release</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\pkey\rsa_verify_pss.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">
   <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid>{95C50864-854C-2A11-4C91-BCE654E344FB}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>rsa_verify_pss</RootNamespace>
 </PropertyGroup>
```

```
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
   <UseDebugLibraries>true</UseDebugLibraries>
   <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
   <UseDebugLibraries>true</UseDebugLibraries>
   <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
    <ConfigurationType>Application</ConfigurationType>
   <UseDebugLibraries>false</UseDebugLibraries>
   <WholeProgramOptimization>true</WholeProgramOptimization>
   <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
   <UseDebugLibraries>false</UseDebugLibraries>
   <WholeProgramOptimization>true</WholeProgramOptimization>
   <CharacterSet>Unicode</CharacterSet>
   <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')"
 Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup
 Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <LinkIncremental>true</LinkIncremental>
```

```
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>

<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
```

```
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
```

```
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
   </Link>
 </ItemDefinitionGroup>
  <Import Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDQwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDUwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQEdT0OFf5G
UcrgX2XllCyJzP94NZ464GsgB6psNLsDeL+j7AU+oJy7VLvW/lHh3ODgl08Z9bhq
LFBmNjnHbm8Qo4GJMIGGMB0GA1UdDgQWBBTXh06MAV9S4l4lG1TKOrKRBh4qnzBX
BgNVHSMEUDBOgBQox4F1NsZunlsduoGvzIgRSYfB36EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAzggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAIW++zqDZlLLUk/emePohdNOp5JO3wS9
XvkBJ6Wua7GBAiAdx+EKmdjVrwnzrQltTgnmSfGMXhKNYifK3uD83W3pcQ==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDMwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDQwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQUXDgcUVNT
9hovbZE5HL6rjOb7C55wEuWKThV/CcZ4rWrXx7VXHYdD/R3aDA7JSvYpm2sTok4i
sblDzhZM/GDNo4GJMIGGMB0GA1UdDgQWBBQox4F1NsZunlsduoGvzIgRSYfB3zBX
BgNVHSMEUDBOgBQApzZdtBdD3dLxouQpr/aDiVttd6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAyggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgAkiNhqFAZXSUWEDK91OZvQGdeZOtd6mC
+Wv3fGk3t28CIEKOwidkUTUaiPdZ4efmAr+CEeGzdq27ob2S+nqqHqgV
-----END
 CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDIwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDMwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQRDXDNIi1p
ereudhqwa2LslXgsxnB63Hu5y5lg+1WPruIYPzD/Ho0APveVdzFLVji19+bE4+tF
PYL1SpsN1WfWo4GJMIGGMB0GA1UdDgQWBBQApzZdtBdD3dLxouQpr/aDiVttdzBX
BgNVHSMEUDBOgBT5RCgQ0AlZTQbfFB2+6+w0XRvydaEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAxggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAOnd+7bAofkHVa4KFNjv3TCegw1lrhuM
8Of8wgvrTEGoAiEAsS8iKMpSfXH4D0egg4gLamE6akde965rDtySU+ve9lg=
-----END
 CERTIFICATE-----
-----BEGIN CERTIFICATE-----
```

MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDEwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDIwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQWHpv1i6lf
wvNPOP5ka6S0n55EvzoaYK6pbTXP6yMOW/4XZSPKx5Zoq4FMe0cKzGIIFL1rzj1V
2czYB+qvLhyio4GJMIGGMB0GA1UdDgQWBBT5RCgQ0AlZTQbfFB2+6+w0XRvydTBX
BgNVHSMEUDBOgBSh3uHkX5nj86yFEFwjscSWM40P+qEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAI7unGW/gr9tOc3i+dF5N815srgh+FrX
oj9Et74EcSpTAiBubv+vOH0DE0gmYI11HeAIgutWqqMIC72dZlwTF/Vi3g==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB3jCCAYWgAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDAwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQznn9zHHwL
GO8VR4W9V7vMlxCdoojzEOiX5Y6JtPtFOz866ueHY6zoN0/mJ6DnqnSXilJIUUeW
6eGfqmka7nxko4GRMIGOMB0GA1UdDgQWBBSh3uHkX5nj86yFEFwjscSWM40P+jBf
BgNVHSMEWDBWgBQlFYvU5WboI4fcdPoiQs8/fPHZraEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggkA/KCWhcqToHAw
DAYDVR0TBAUwAwEB/zAKBggqhkjOPQQDAgNHADBEAiBasbuinP+pJTU4oDCVD8zQ
1rJBDSOKIEyWu84/D6Hj6wIgVMPUoO01bPhzllAa/gW8Xk/daey09SBgN3AT9pWU
TDA=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIBpTCCAUugAwIBAgIJAPygloXKk6BwMAoGCCqGSM49BAMCMC8xCzAJBgNVBAYT
AlVLMREwDwYDVQQKDAhtYmVkIFRMUzENMAsGA1UEAwwEQ0EwMDAeFw0xNzA2MjIx
MTUwMzJaFw0yNzA2MjMxMTUwMzJaMC8xCzAJBgNVBAYTAlVLMREwDwYDVQQKDAht
YmVkIFRMUzENMAsGA1UEAwwEQ0EwMDBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IA
BFW41/qAwAPpy+Txdc7PKmzZsq9CPiujKU4vpF1ekXnGx2HP420QobwBVVWhkzRm
LwdboH2j65dcCKjQ7mv/dxKjUDBOMB0GA1UdDgQWBBQlFYvU5WboI4fcdPoiQs8/
fPHZrTAfBgNVHSMEGDAWgBQlFYvU5WboI4fcdPoiQs8/fPHZrTAMBgNVHRMEBTAD
AQH/MAoGCCqGSM49BAMCA0gAMEUCIQC7iRcVzwMyfVK5imirJ7MqJQ04euH4CLOt
IZ+SNfaERAIgSU0MWFDosVEIpg8YMqIHeF7Mg4ZyH6+fGazJgVLttUY=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIBzTCCAVOgAwIBAgIJAODh6PAeD9/vMAoGCCqGSM49BAMCMD4xCzAJBgNVBAYT
Ak5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBF
QyBDQTAeFw0xNDA0MDkxMTIzNTRaFw0yNDA0MDYxMTIzNTRaMD4xCzAJBgNVBAYT
Ak5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBF
QyBDQTB2MBAGByqGSM49AgEGBSuBBAAiA2IABMPaKzRBN1gvh1b+/Im6KUNLTuBu
ww5XUzM5WNRStJGVOQsj318XJGJI/BqVKc4sLYfCiFKAr9ZqqyHduNMcbli4yuiy
aY7zQa0pw7RfdadHb9UZKVVpmlM7ILRmFmAzHqMdMBswDAYDVR0TBAUwAwEB/zAL
BgNVHQ8EBAMCAgQwCgYIKoZIzj0EAwIDaAAwZQIwGGlbynd1jU3WkUx6Irhk9Lob
z2B+1eIO6+eu3En8B3rh8Ipfxo0e0hpfaRFYP1MUAjEAjxxBchRWJAzZ6/47Wg/7
UoasRINgP5B/uJhTnftS1bqyuWHastb4LW5/YLOvPbMQ

-----END CERTIFICATE-----
N =
A1D46FBA2318F8DCEF16C280948B1CF27966B9B47225ED2989F8D74B45BD36049C0AAB5AD0FF003553B
A843C8E12782FC5873BB89A3DC84B883D25666CD22BF3ACD5B675969F8BEBFBCAC93FDD927C7442B17
8B10D1DFF9398E52316AAE0AF74E594650BDC3C670241D418684593CDA1A7B9DC4F20D2FDC6F6634407
4003E211
E = 010001
D =
589552BB4F2F023ADDDD5586D0C8FD857512D82080436678D07F984A29D892D31F1F7000FC5A39A0F73E
27D885E47249A4148C8A5653EF69F91F8F736BA9F84841C2D99CD8C24DE8B72B5C9BE0EDBE23F93D7317
49FEA9CFB4A48DD2B7F35A2703E74AA2D4DB7DE9CEEA7D763AF0ADA7AC176C4E9A22C4CDA65CEC0
C65964401
P =
CD083568D2D46C44C40C1FA0101AF2155E59C70B08423112AF0C1202514BBA5210765E29FF13036F56C749
5894D80CF8C3BAEE2839BACBB0B86F6A2965F60DB1
Q =
CA0EEEA5E710E8E9811A6B846399420E3AE4A4C16647E426DDF8BBBCB11CD3F35CE2E4B6BCAD07AE2
C0EC2ECBFCC601B207CDD77B5673E16382B1130BF465261
DP =
0D0E21C07BF434B4A83B116472C2147A11D8EB98A33CFBBCF1D275EF19D815941622435AAF3839B6C432
CA53CE9E772CFBE1923A937A766FD93E96E6EDEC1DF1
DQ =
269CEBE6305DFEE4809377F078C814E37B45AE6677114DFC4F76F5097E1F3031D592567AC55B9B98213B40
ECD54A4D2361F5FAACA1B1F51F71E4690893C4F081
QP
=
97AC5BB885ABCA314375E9E4DB1BA4B2218C90619F61BD474F5785075ECA81750A735199A8C191FE2D3
355E7CF601A70E5CABDE0E02C2538BB9FB4871540B3C1
AES-128-CBC Encrypt NIST KAT #1
aes_encrypt_cbc:"ffffffffffff80000000000000000000":"00000000000000000000000000000000":"00000000000000
00000000000000000000":"8b527a6aebdaec9eaef8eda2cb7783e5":0

AES-128-CBC Encrypt NIST KAT #2
aes_encrypt_cbc:"ffffffffffffc0000000000000000000":"00000000000000000000000000000000":"00000000000000
00000000000000000000":"43fdaf53ebbc9880c228617d6a9b548b":0

AES-128-CBC Encrypt NIST KAT #3
aes_encrypt_cbc:"ffffffffffffe0000000000000000000":"00000000000000000000000000000000":"00000000000000
00000000000000000000":"53786104b9744b98f052c46f1c850d0b":0

AES-128-CBC Encrypt NIST KAT #4
aes_encrypt_cbc:"e37b1c6aa2846f6fdb413f238b089f23":"00000000000000000000000000000000":"000000000000
0000000000000000000000":"43c9f7e62f5d288bb27aa40ef8fe1ea8":0

AES-128-CBC Encrypt NIST KAT #5
aes_encrypt_cbc:"6c002b682483e0cabcc731c253be5674":"00000000000000000000000000000000":"00000000000
0000000000000000000000":"3580d19cff44f1014a7c966a69059de5":0

AES-128-CBC Encrypt NIST KAT #6
aes_encrypt_cbc:"143ae8ed6555aba96110ab58893a8ae1":"00000000000000000000000000000000":"00000000000000000000000000000000":"806da864dd29d48deafbe764f8202aef":0

AES-128-CBC
Encrypt NIST KAT #7
aes_encrypt_cbc:"00000000000000000000000000000000":"00000000000000000000000000000000":"6a118a874519e64e9963798a503f1d35":"dc43be40be0e53712f7e2bf5ca707209":0

AES-128-CBC Encrypt NIST KAT #8
aes_encrypt_cbc:"00000000000000000000000000000000":"00000000000000000000000000000000":"cb9fceec81286ca3e989bd979b0cb284":"92beedab1895a94faa69b632e5cc47ce":0

AES-128-CBC Encrypt NIST KAT #9
aes_encrypt_cbc:"00000000000000000000000000000000":"00000000000000000000000000000000":"b26aeb1874e47ca8358ff22378f09144":"459264f4798f6a78bacb89c15ed3d601":0

AES-128-CBC Encrypt NIST KAT #10
aes_encrypt_cbc:"00000000000000000000000000000000":"00000000000000000000000000000000":"ffffffffffffffffffffffc000000000":"90684a2ac55fe1ec2b8ebd5622520b73":0

AES-128-CBC Encrypt NIST KAT #11
aes_encrypt_cbc:"00000000000000000000000000000000":"00000000000000000000000000000000":"ffffffffffffffffffffffe000000000":"7472f9a7988607ca79707795991035e6":0

AES-128-CBC
Encrypt NIST KAT #12
aes_encrypt_cbc:"00000000000000000000000000000000":"00000000000000000000000000000000":"ffffffffffffffffffffffff000000000":"56aff089878bf3352f8df172a3ae47d8":0

AES-128-CBC Decrypt NIST KAT #1
aes_decrypt_cbc:"fffffffe000000000000000000000000":"00000000000000000000000000000000":"23f710842b9bb9c32f26648c786807ca":"00000000000000000000000000000000":0

AES-128-CBC Decrypt NIST KAT #2
aes_decrypt_cbc:"fffffffff000000000000000000000000":"00000000000000000000000000000000":"44a98bf11e163f632c47ec6a49683a89":"00000000000000000000000000000000":0

AES-128-CBC Decrypt NIST KAT #3
aes_decrypt_cbc:"fffffffff800000000000000000000000":"00000000000000000000000000000000":"0f18aff94274696d9b61848bd50ac5e5":"00000000000000000000000000000000":0

AES-128-CBC Decrypt NIST KAT #4
aes_decrypt_cbc:"e234cdca2606b81f29408d5f6da21206":"00000000000000000000000000000000":"fff60a4740086b3b9c56195b98d91a7b":"00000000000000000000000000000000":0

AES-128-CBC

Decrypt NIST KAT #5
aes_decrypt_cbc:"13237c49074a3da078dc1d828bb78c6f":"00000000000000000000000000000000":"8146a08e2357f0caa30ca8c94d1a0544":"00000000000000000000000000000000":0

AES-128-CBC Decrypt NIST KAT #6
aes_decrypt_cbc:"3071a2a48fe6cbd04f1a129098e308f8":"00000000000000000000000000000000":"4b98e06d356deb07ebb824e5713f7be3":"00000000000000000000000000000000":0

AES-128-CBC Decrypt NIST KAT #7
aes_decrypt_cbc:"00000000000000000000000000000000":"00000000000000000000000000000000":"0336763e966d92595a567cc9ce537f5e":"f34481ec3cc627bacd5dc3fb08f273e6":0

AES-128-CBC Decrypt NIST KAT #8
aes_decrypt_cbc:"00000000000000000000000000000000":"00000000000000000000000000000000":"a9a1631bf4996954ebc093957b234589":"9798c4640bad75c7c3227db910174e72":0

AES-128-CBC Decrypt NIST KAT #9
aes_decrypt_cbc:"00000000000000000000000000000000":"00000000000000000000000000000000":"ff4f8391a6a40ca5b25d23bedd44a597":"96ab5c2ff612d9dfaae8c31f30c42168":0

AES-128-CBC
Decrypt NIST KAT #10
aes_decrypt_cbc:"00000000000000000000000000000000":"00000000000000000000000000000000":"f9b0fda0c4a898f5b9e6f661c4ce4d07":"fffffffffffffffffffffffffffffff0":0

AES-128-CBC Decrypt NIST KAT #11
aes_decrypt_cbc:"00000000000000000000000000000000":"00000000000000000000000000000000":"8ade8959136 85c67c5269f8aae42983e":"fffffffffffffffffffffffffffffff8":0

AES-128-CBC Decrypt NIST KAT #12
aes_decrypt_cbc:"00000000000000000000000000000000":"00000000000000000000000000000000":"39bde67d5c8ed8a8b1c37eb8fa9f5ac0":"fffffffffffffffffffffffffffffffc":0

AES-192-CBC Encrypt NIST KAT #1
aes_encrypt_cbc:"fffffffffffffffffffffffffffffffffffffffffffffe00":"00000000000000000000000000000000":"00000000000000000000000000000000":"ddb505e6cc1384cbaec1df90b80beb20":0

AES-192-CBC Encrypt NIST KAT #2
aes_encrypt_cbc:"fffffffffffffffffffffffffffffffffffffffffffffff00":"00000000000000000000000000000000":"00000000000000000000000000000000":"5674a3bed27bf4bd3622f9f5fe208306":0

AES-192-CBC
Encrypt NIST KAT #3
aes_encrypt_cbc:"fffffffffffffffffffffffffffffffffffffffffffffff80":"00000000000000000000000000000000":"00000000000000000000000000000000":"b687f26a89cfbfbb8e5eeac54055315e":0

AES-192-CBC Encrypt NIST KAT #4
aes_encrypt_cbc:"25a39dbfd8034f71a81f9ceb55026e4037f8f6aa30ab44ce":"00000000000000000000000000000000

0":"00000000000000000000000000000000":"3608c344868e94555d23a120f8a5502d":0

AES-192-CBC Encrypt NIST KAT #5
aes_encrypt_cbc:"e08c15411774ec4a908b64eadc6ac4199c7cd453f3aaef53":"00000000000000000000000000000000
0":"00000000000000000000000000000000":"77da2021935b840b7f5dcc39132da9e5":0

AES-192-CBC Encrypt NIST KAT #6
aes_encrypt_cbc:"3b375a1ff7e8d44409696e6326ec9dec86138e2ae010b980":"00000000000000000000000000000000
00":"00000000000000000000000000000000":"3b7c24f825e3bf9873c9f14d39a0e6f4":0

AES-192-CBC Encrypt NIST KAT #7
aes_encrypt_cbc:"0000000000000000000000000000000000000000000000000000":"00000000000000000000000000000000
0000":"51719783d3185a535bd75adc65071ce1":"4f354592ff7c8847d2d0870ca9481b7c":0

AES-192-CBC
Encrypt NIST KAT #8
aes_encrypt_cbc:"0000000000000000000000000000000000000000000000000000":"00000000000000000000000000000000
0000":"26aa49dcfe7629a8901a69a9914e6dfd":"d5e08bf9a182e857cf40b3a36ee248cc":0

AES-192-CBC Encrypt NIST KAT #9
aes_encrypt_cbc:"0000000000000000000000000000000000000000000000000000":"00000000000000000000000000000000
0000":"941a4773058224e1ef66d10e0a6ee782":"067cd9d3749207791841562507fa9626":0

AES-192-CBC Encrypt NIST KAT #10
aes_encrypt_cbc:"0000000000000000000000000000000000000000000000000000":"00000000000000000000000000000000
0000":"ffc00000000000000000000000000000":"030d7e5b64f380a7e4ea5387b5cd7f49":0

AES-192-CBC Encrypt NIST KAT #11
aes_encrypt_cbc:"0000000000000000000000000000000000000000000000000000":"00000000000000000000000000000000
0000":"ffe00000000000000000000000000000":"0dc9a2610037009b698f11bb7e86c83e":0

AES-192-CBC Encrypt NIST KAT #12
aes_encrypt_cbc:"0000000000000000000000000000000000000000000000000000":"00000000000000000000000000000000
0000":"fff00000000000000000000000000000":"0046612c766d1840c226364f1fa7ed72":0

AES-192-CBC
Decrypt NIST KAT #1
aes_decrypt_cbc:"0000000000000000000000000000000000000000000000000000":"00000000000000000000000000000000
0000":"902d88d13eae52089abd6143cfe394e9":"ffffffffe00000000000000000000000":0

AES-192-CBC Decrypt NIST KAT #2
aes_decrypt_cbc:"0000000000000000000000000000000000000000000000000000":"00000000000000000000000000000000
0000":"d49bceb3b823fedd602c305345734bd2":"fffffffff00000000000000000000000":0

AES-192-CBC Decrypt NIST KAT #3
aes_decrypt_cbc:"0000000000000000000000000000000000000000000000000000":"00000000000000000000000000000000
0000":"707b1dbb0ffa40ef7d95def421233fae":"fffffffff80000000000000000000000":0

AES-192-CBC Decrypt NIST KAT #4
aes_decrypt_cbc:"ffffffffffffffffffffffc0000000000000000000000000000000":"00000000000000000000000000000000":"
8dfd999be5d0cfa35732c0ddc88ff5a5":"00000000000000000000000000000000":0

AES-192-CBC Decrypt NIST KAT #5
aes_decrypt_cbc:"ffffffffffffffffffffffe0000000000000000000000000000000":"00000000000000000000000000000000":"
02647c76a300c3173b841487eb2bae9f":"00000000000000000000000000000000":0

AES-192-CBC
Decrypt NIST KAT #6
aes_decrypt_cbc:"fffffffffffffffffffff8000000000000000000000000000000":"00000000000000000000000000000000":"1
72df8b02f04b53adab028b4e01acd87":"00000000000000000000000000000000":0

AES-192-CBC Decrypt NIST KAT #7
aes_decrypt_cbc:"b3ad5cea1dddc214ca969ac35f37dae1a9a9d1528f89bb35":"0000000000000000000000000000000000
00":"3cf5e1d21a17956d1dffad6a7c41c659":"00000000000000000000000000000000":0

AES-192-CBC Decrypt NIST KAT #8
aes_decrypt_cbc:"45899367c3132849763073c435a9288a766c8b9ec2308516":"0000000000000000000000000000000000
000":"69fd12e8505f8ded2fdcb197a121b362":"00000000000000000000000000000000":0

AES-192-CBC Decrypt NIST KAT #9
aes_decrypt_cbc:"ec250e04c3903f602647b85a401a1ae7ca2f02f67fa4253e":"0000000000000000000000000000000000
0":"8aa584e2cc4d17417a97cb9a28ba29c8":"00000000000000000000000000000000":0

AES-192-CBC Decrypt NIST KAT #10
aes_decrypt_cbc:"0000000000000000000000000000000000000000000000000000":"0000000000000000000000000000000000
0000":"c9b8135ff1b5adc413dfd053b21bd96d":"9c2d8842e5f48f57648205d39a239af1":0

AES-192-CBC
Decrypt NIST KAT #11
aes_decrypt_cbc:"0000000000000000000000000000000000000000000000000000":"0000000000000000000000000000000000
0000":"4a3650c3371ce2eb35e389a171427440":"bff52510095f518ecca60af4205444bb":0

AES-192-CBC Decrypt NIST KAT #12
aes_decrypt_cbc:"0000000000000000000000000000000000000000000000000000":"0000000000000000000000000000000000
0000":"4f354592ff7c8847d2d0870ca9481b7c":"51719783d3185a535bd75adc65071ce1":0

AES-256-CBC Encrypt NIST KAT #1
aes_encrypt_cbc:"8000000000000000000000000000000000000000000000000000000000000000":"000000000000
0000000000000000000000":"00000000000000000000000000000000":"e35a6dcb19b201a01ebcfa8aa22b5759":0

AES-256-CBC Encrypt NIST KAT #2
aes_encrypt_cbc:"c0000000000000000000000000000000000000000000000000000000000000000":"000000000000
0000000000000000000000":"00000000000000000000000000000000":"b29169cdcf2d83e838125a12ee6aa400":0

AES-256-CBC

Encrypt NIST KAT #3
aes_encrypt_cbc:"e0000000000000000000000000000000000000000000000000000000000000000000":"000000000000000000000000000000000000":"00000000000000000000000000000000":"d8f3a72fc3cdf74dfaf6c3e6b97b2fa6":0

AES-256-CBC Encrypt NIST KAT #4
aes_encrypt_cbc:"dc0eba1f2232a7879ded34ed8428eeb8769b056bbaf8ad77cb65c3541430b4cf":"000000000000000000000000000000000000":"00000000000000000000000000000000":"fc6aec906323480005c58e7e1ab004ad":0

AES-256-CBC Encrypt NIST KAT #5
aes_encrypt_cbc:"f8be9ba615c5a952cabbca24f68f8593039624d524c816acda2c9183bd917cb9":"000000000000000000000000000000000000":"00000000000000000000000000000000":"a3944b95ca0b52043584ef02151926a8":0

AES-256-CBC Encrypt NIST KAT #6
aes_encrypt_cbc:"797f8b3d176dac5b7e34a2d539c4ef367a16f8635f6264737591c5c07bf57a3e":"000000000000000000000000000000000000":"00000000000000000000000000000000":"a74289fe73a4c123ca189ea1e1b49ad5":0

AES-256-CBC Encrypt NIST KAT #7
aes_encrypt_cbc:"0000000000000000000000000000000000000000000000000000000000000000000000":"000000000000000000000000000000000000":"761c1fe41a18acf20d241650611d90f1":"623a52fcea5d443e48d9181ab32c7421":0

AES-256-CBC
Encrypt NIST KAT #8
aes_encrypt_cbc:"0000000000000000000000000000000000000000000000000000000000000000000000":"000000000000000000000000000000000000":"8a560769d605868ad80d819bdba03771":"38f2c7ae10612415d27ca190d27da8b4":0

AES-256-CBC Encrypt NIST KAT #9
aes_encrypt_cbc:"0000000000000000000000000000000000000000000000000000000000000000000000":"000000000000000000000000000000000000":"91fbef2d15a97816060bee1feaa49afe":"1bc704f1bce135ceb810341b216d7abe":0

AES-256-CBC Encrypt NIST KAT #10
aes_encrypt_cbc:"0000000000000000000000000000000000000000000000000000000000000000000000":"000000000000000000000000000000000000":"ffffffffffffff800000000000000000":"0d9ac756eb297695eed4d382eb126d26":0

AES-256-CBC Encrypt NIST KAT #11
aes_encrypt_cbc:"0000000000000000000000000000000000000000000000000000000000000000000000":"000000000000000000000000000000000000":"fffffffffffffc00000000000000000":"56ede9dda3f6f141bff1757fa689c3e1":0

AES-256-CBC
Encrypt NIST KAT #12
aes_encrypt_cbc:"0000000000000000000000000000000000000000000000000000000000000000000000":"000000000000000000000000000000000000":"fffffffffffffe00000000000000000":"768f520efe0f23e61d3ec8ad9ce91774":0

AES-256-CBC Decrypt NIST KAT #1
aes_decrypt_cbc:"0000000000000000000000000000000000000000000000000000000000000000000000":"000000000000000000000000000000000000":"49af6b372135acef10132e548f217b17":"ff000000000000000000000000000000":0

AES-256-CBC Decrypt NIST KAT #2
aes_decrypt_cbc:"0000000000000000000000000000000000000000000000000000000000000000000000":"000000000000

00000000000000000000":"8bcd40f94ebb63b9f7909676e667f1e7":"ff800000000000000000000000000000":0

AES-256-CBC Decrypt NIST KAT #3
aes_decrypt_cbc:"0000000000000000000000000000000000000000000000000000000000000000":"0000000000000000000000000000000000":"fe1cffb83f45dcfb38b29be438dbd3ab":"ffc00000000000000000000000000000":0

AES-256-CBC Decrypt NIST KAT #4
aes_decrypt_cbc:"ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffc00":"00000000000000000000000000000000"
:"cca7c3086f5f9511b31233da7cab9160":"00000000000000000000000000000000":0

AES-256-CBC
Decrypt NIST KAT #5
aes_decrypt_cbc:"fffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffe00":"00000000000000000000000000000000"
:"5b40ff4ec9be536ba23035fa4f06064c":"00000000000000000000000000000000":0

AES-256-CBC Decrypt NIST KAT #6
aes_decrypt_cbc:"fffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff00":"00000000000000000000000000000000":
"60eb5af8416b257149372194e8b88749":"00000000000000000000000000000000":0

AES-256-CBC Decrypt NIST KAT #7
aes_decrypt_cbc:"90143ae20cd78c5d8ebdd6cb9dc1762427a96c78c639bccc41a61424564eafe1":"00000000000000000000000000000000":"798c7c005dee432b2c8ea5dfa381ecc3":"00000000000000000000000000000000":0

AES-256-CBC Decrypt NIST KAT #8
aes_decrypt_cbc:"b7a5794d52737475d53d5a377200849be0260a67a2b22ced8bbef12882270d07":"0000000000000000000000000000000000":"637c31dc2591a07636f646b72daabbe7":"00000000000000000000000000000000":0

AES-256-CBC
Decrypt NIST KAT #9
aes_decrypt_cbc:"fca02f3d5011cfc5c1e23165d413a049d4526a991827424d896fe3435e0bf68e":"000000000000000000000000000000000":"179a49c712154bbffbe6e7a84a18e220":"00000000000000000000000000000000":0

AES-256-CBC Decrypt NIST KAT #10
aes_decrypt_cbc:"0000000000000000000000000000000000000000000000000000000000000000":"0000000000000000000000000000000000":"5c9d844ed46f9885085e5d6a4f94c7d7":"014730f80ac625fe84f026c60bfd547d":0

AES-256-CBC Decrypt NIST KAT #11
aes_decrypt_cbc:"0000000000000000000000000000000000000000000000000000000000000000":"0000000000000000000000000000000000":"a9ff75bd7cf6613d3731c77c3b6d0c04":"0b24af36193ce4665f2825d7b4749c98":0

AES-256-CBC Decrypt NIST KAT #12
aes_decrypt_cbc:"0000000000000000000000000000000000000000000000000000000000000000":"0000000000000000000000000000000000":"623a52fcea5d443e48d9181ab32c7421":"761c1fe41a18acf20d241650611d90f1":0
-----BEGIN CERTIFICATE-----
MIIDPzCCAiegAwIBAgIBATANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTEwMjEyMTQ0NDA2WhcNMjEwMjEyMTQ0NDA2WjA8MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxGjAYBgNVBAMTEVBvbGFyU1NMIFNlcnZlciAxMIIBIjAN

BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqQIfPUBq1VVTi/027oJlLhVhXom/
uOhFkNvuiBZS0/FDUEeWEllkh2v9K+BG+XO+3c+S4ZFb7Wagb4kpeUWA0INq1UFD
d185fAkER4KwVzlw7aPsFRkeqDMIR8EFQqn9TMO0390GH00QUUBncxMPQPhtgSVf
CrFTxjB+FTms+Vruf5KepgVb5xOXhbUjktnUJAbVCSWJdQfdphqPPwkZvq1lLGTr
lZvc/kFeF6babFtpzAK6FCwWJJxK3M3Q91Jnc/EtoCP9fvQxyi1wyokLBNsupk9w
bp7OvViJ4lNZnm5akmXiiD8MlBmj3eXonZUT7Snbq3AS3FrKaxerUoJUsQIDAQAB
o00wSzAJBgNVHRMEAjAAMB0GA1UdDgQWBBQfdNY/KcF0dEU7BRIsPai9Q1kCpjAf
BgNVHSMEGDAWgBS0WuSls97SUva51aaVD+s+vMf9/zANBgkqhkiG9w0BAQUFAAOC
AQEAvc+WwZUemsJu2IiI2Cp6liA+UAvIx98dQe3kZs2zAoF9VwQbXcYzWQ/BILkj
NImKbPL9x0g2jIDn4ZvGYFywMwIO/d++YbwYiQw42/v7RiMy94zBPnzeHi86dy/0
jpOOJUx3IXRsGLdyjb/1T11klcFqGnARiK+8VYolMPP6afKvLXX7K4kiUpsFQhUp
E5VeM5pV1Mci2ETOJau2cO40FJvI/C9W/wR+GAArMaw2fxG77E3laaa0LAOlexM6
A4KOb5f5cGTM5Ih6tEF5FVq3/9vzNIYMa1FqzacBLZF8zSHYLEimXBdzjBoN4qDU
/WzRyYRBRjAI49mzHX6raleqnw==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDhzCCAm+gAwIBAgIBADANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTEwMjEyMTQ0NDAwWhcNMjEwMjEyMTQ0NDAwWjA7MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDA3zf8F7vglp0/ht6WMn1EpRagzSHx
mdTs6st8GFgIlKXsm8WL3xoemTiZhx57wI053zhdcHgH057Zk+i5clHFzqMwUqny
50BwFMtEonILwuVA+T7lpg6z+exKY8C4KQB0nFc7qKUEkHHxvYPZP9al4jwqj+8n
YMPGn8u67GB9t+aEMr5P+1gmIgNb1LTV+/Xjli5wwOQuvfwu7uJBVcA0Ln0kcmnL
R7EUQIN9Z/SG9jGr8XmksrUuEvmEF/Bibyc+E1ixVA0hmnM3oTDPb5Lc9un8rNsu
KNF+AksjoBXyOGVkCeoMbo4bF6BxyLObyavpw/LPh5aPgAIynplYb6LVAgMBAAGj
gZUwgZIwDAYDVR0TBAUwAwEB/zAdBgNVHQ4EFgQUtFrkpbPe0lL2udWmlQ/rPrzH
/f8wYwYDVR0jBFwwWoAUtFrkpbPe0lL2udWmlQ/rPrzH/f+hP6Q9MDsxCzAJBgNV
BAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEZMBcGA1UEAxMQUG9sYXJTU0wgVGVz
dCBDQYIBADANBgkqhkiG9w0BAQUFAAOCAQEAuP1U2ABUkIslsCfdlc2i94QHHYeJ
SsR4EdgHtdciUI5I62J6Mom+Y0dT/7a+8S6MVMCZP6C5NyNyXw1GWY/YR82XTJ8H
DBJiCTok5DbZ6SzaONBzdWHXwWwmi5vg1dxn7YxrM9d0IjxM27WNKs4sDQhZBQkF
pjmfs2cb4oPl4Y9T9meTx/lvdkRYEug61Jfn6cA+qHpyPYdTH+UshITnmp5/Ztkf
m/UTSLBNFNHesiTZeH31NcxYGdHSme9Nc/gfidRa0FLOCfWxRlFqAI47zG9jAQCZ
7Z2mCGDNMhjQc+BYcdnl0lPXjdDK6V0qCg1dVewhUBcW5gZKzV7e9+DpVA==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE REQUEST-----
MIIBzTCCAQYCAQAwNDELMAkGA1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NMMRIw
EAYDVQQDEwlsb2NhbGhvc3QwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAN0R
ip+ZurBoyirqO2ptWZftTslU5A3uzqB9oB6q6A7CuxNA24oSjokTJKXF9frY9ZDX
yMrLxf6THa/aEiNzUnlGGrqgVyt2FjGzqK/nOJsIi2OZOgol7kXSGFi6uZMa7dRY
mmMbN/z3FAifhWVJ81kybdHg6G3eUu1mtKkL2kCVAgMBAAGgKTAnBgkqhkiG9w0B
CQ4xGjAYMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgXgMD0GCSqGSIb3DQEBCjAwoA0w
CwYJYIZIAWUDBAIEoRowGAYJKoZIhvcNAQEIMAsGCWCGSAFlAwQCBKIDAgFiA4GB
AMlYYZKqpDqg5UZZq3NB3QUR9qftY/52/0gPfruw5s2gNtFmG1uyEBJX/oc7C/fU
lxo74HDraWJyvP7c3MMhOuwr/RfPNQhA2Hgwz9RuJIBhQrJfiZuHsCfiKVofMuMf

ar/4EKfyoELDdilhg6i+abahGOkqyXsjavFtyDSeCpXH
-----END CERTIFICATE REQUEST-----
-----BEGIN X509 CRL-----
MIIBqzCBlDANBgkqhkiG9w0BAQsFADA7MQswCQYDVQQGEwJOTDERMA8GA1UEChMI
UG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EXDTExMDIxMjE0NDQw
N1oXDTExMDQxMzE0NDQwN1owKDASAgEBFw0xMTAyMTIxNDQ0MDdaMBICAQMXDTEx
MDIxMjE0NDQwN1owDQYJKoZIhvcNAQELBQADggEBAG4mBBgwfNynCYYL2CEnqore
mgKpC32tB6WiUBu9figcvdN3nSX/1wrB8rpiE8R04C8oSFglwhotJCnlWsy42tjb
0pk0Wuizln0PFMc/OypqRNNhwx31SHH42W4KzONiqvq3n/WkH3M1YniR1ZnMlyvi
lJioQn6ZAoc6O6mMP1J9duKYYhiMAOV992PD1/iqXw+jYN31RwdIS8/mGzIs4ake
EdviwhM3E4/sVbNOWCOnZFYV4m+yNAEe29HL1VKw6UXixBczct+brqXNVD3U6T0F
5ovR6BTefZO17eT52Duke5RZGDUyQOGywxOYKI5W+FcOYdp+U5Idk399tAz2Mdw=
-----END X509 CRL-----
-----BEGIN CERTIFICATE-----
MIIDBTCCAeegAwIBAgIBFjATBgkqhkiG9w0BAQowBqIEAgIA6jA7MQswCQYDVQQG
EwJOTDERMA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3Qg
Q0EwHhcNMTQwMTIwMTMzODE2WhcNMjQwMTE4MTMzODE2WjA0MQswCQYDVQQGEwJO
TDERMA8GA1UEChMIUG9sYXJTU0wxEjAQBgNVBAMTCWxvY2FsaG9zdDCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA3RGKn5m6sGjKKuo7am1Zl+1OyVTkDe7OoH2g
HqroDsK7E0DbihKOiRMkpcX1+tj1kNfIysvF/pMdr9oSI3NSeUYauqBXK3YWMbOo
r+c4mwiLY5k6CiXuRdIYWLq5kxrt1FiaYxs3/PcUCJ+FZUnzWTJt0eDobd5S7Wa0
qQvaQJUCAwEAAaOBkjCBjzAJBgNVHRMEAjAAMB0GA1UdDgQWBBTu88f1HxWlTUeJ
wdMiY7Lfp869UTBjBgNVHSMEXDBagBS0WuSls97SUva51aaVD+s+vMf9/6E/pD0w
OzELMAkGA1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NMMRkwFwYDVQQDExBQb2xh
clNTTCBUZXN0IENBggEAMBMGCSqGSIb3DQEBCjAGogQCAgDqA4IBAQDAog/jXydR
vDIugTzBXtfVK0CEX8iyQ4cVzQmXWSne8204v943K5D2hktSBkjdQUdcnVvVgLR6
te50jV89ptN/NofX+fo9fhSRN9vGgQVWzOOFiO0zcThy749pirJu1Kq5OJdthIyW
Pu0UCz5G0k3kTp0JPevGlsNc8S9Ak1tFuB0IPJjrbfODWHS2LDuO+dB6gpkNTdrj
88ogYtBsN4D5gsXBRUfobXokUwejBwLrD6XwyQx+0bMwSCxgHEhxvuUkx1vdlXGw
JG3aF92u8mIxoKSAPaPdqy930mQvmpUWcN5Y1IMbtEGoQCKMYgosFcazJpJcjnX1
o4Hl/lqjwCEG
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIBqDCCAUygAwIBAgIBUjAMBggqhkjOPQQDAgUAMDExDzANBgNVBAMTBlJvb3Qg
ODERMA8GA1UEChMIbWJlZCBUTFMxCzAJBgNVBAYTAlVLMB4XDTAxMDEwMTAwMDAw
MFoXDTMwMTIzMTIzNTk1OVowMTEPMA0GA1UEAxMGSW50IDgyMREwDwYDVQQKEwht
YmVkIFRMUzELMAkGA1UEBhMCVUswWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAS2
giYQt4HVfQ2t8eTS0bvISwp7ol2x17umbllBxwzGDFEUQ00JL1/SStezecK0lNhE
0AvY8Ez2soQEtdSeQGkCo1MwUTAPBgNVHRMECDAGAQH/AgEAMB0GA1UdDgQWBBS3
+nsv3nQknSg4aDjlTiRpCPo7XzAfBgNVHSMEGDAWgBTHFA2hAu0tPnzeYnLcmlTQ
j4FAajAMBggqhkjOPQQDAgUAA0gAMEUCIQDus2Lvx3yyvaViY1s334uMm6ge484X
oktMyxLVjkAMiAIgehTHiJJaT9PnlVa+hUpxsIfVAuMexrm5fw/bDF5Nxzw=
-----END CERTIFICATE-----
Arguments with no value
mpi_null:

Base test mpi_read_write_string #1

mpi_read_write_string:10:"128":10:"128":100:0:0

Base test mpi_read_write_string #2
mpi_read_write_string:10:"128":16:"80":100:0:0

Base test mpi_read_write_string #3 (Read zero)
mpi_read_write_string:10:"0":10:"0":100:0:0

Base test mpi_read_write_string #3 (Negative decimal)
mpi_read_write_string:10:"-23":10:"-23":100:0:0

Base test mpi_read_write_string #3 (Negative hex)
mpi_read_write_string:16:"-20":10:"-32":100:0:0

Base test mpi_read_write_string #3 (Negative decimal)
mpi_read_write_string:16:"-23":16:"-23":100:0:0

Test mpi_read_write_string #1 (Invalid character)
mpi_read_write_string:10:"a28":0:"":100:MBEDTLS_ERR_MPI_INVALID_CHARACTER:0

Test mpi_read_write_string #2 (Illegal input radix)
mpi_read_write_string:19:"a28":0:"":100:MBEDTLS_ERR_MPI_BAD_INPUT_DATA:0

Test mpi_read_write_string #3 (Buffer just fits)
mpi_read_write_string:16:"-23":16:"-23":4:0:0

Test mpi_read_write_string #4 (Buffer too small)
mpi_read_write_string:16:"-23":16:"-23":3:0:MBEDTLS_ERR_MPI_BUFFER_TOO_SMALL

Test
mpi_read_write_string #5 (Illegal output radix)
mpi_read_write_string:16:"-23":17:"-23":4:0:MBEDTLS_ERR_MPI_BAD_INPUT_DATA

Test mpi_read_write_string #6 (Output radix of 15)
mpi_read_write_string:10:"29":15:"1e":100:0:0

Test mpi_read_write_string #7
mpi_read_write_string:10:"561256809817522823341418963203724894906139636935563925208160178921113506041116976827054983195120490405166988278292920768080069408739749795845270734810126360163539134623767555567200198311873649935879019527573078308965316787277179 24":16:"0941379d00fed1491fe15df284dfde4a142f68aa8d412023195cee66883e6290ffe703f4ea5963bf212713cee46b107c09182b5edcd955adac418bf4918e2889af48e1099d513830cec85c26ac1e158b52620e33ba8692f893efbb2f958b4424":200:0:0

Test mpi_read_write_string #8 (Empty MPI -> hex)
mpi_read_write_string:16:"":16:"00":4:0:0

Test mpi_read_write_string #9 (Empty MPI -> dec)
mpi_read_write_string:16:"":10:"0":4:0:0

Test mpi_write_string
#10 (Negative hex with odd number of digits)
mpi_read_write_string:16:"-1":16:"":3:0:MBEDTLS_ERR_MPI_BUFFER_TOO_SMALL

Base test mbedtls_mpi_read_binary #1
mbedtls_mpi_read_binary:"0941379d00fed1491fe15df284dfde4a142f68aa8d412023195cee66883e6290ffe703f4ea5963bf212713cee46b107c09182b5edcd955adac418bf4918e2889af48e1099d513830cec85c26ac1e158b52620e33ba8692f893efbb2f958b4424":10:"561256809817522823341418963203724894906139636935563925208160178921113506041116976827054983195120490405166988278292920768080069408739749795845270734810126360163539134623767555567200198311873649935879019527573078308965316787277179 24"

Base test mbedtls_mpi_write_binary #1
mbedtls_mpi_write_binary:10:"561256809817522823341418963203724894906139636935563925208160178921113506041116976827054983195120490405166988278292920768080069408739749795845270734810126360163539134623767555567200198311873649935879019527573078308965316787277179 24":"0941379d00fed1491fe15df284dfde4a142f68aa8d412023195cee66883e6290ffe703f4ea5963bf212713cee46b107c09182b5edcd955adac418bf4918e2889af48e1099d513830cec85c26ac1e158b52620e33ba8692f893efbb2f958b4424":200:0

Test
mbedtls_mpi_write_binary #1 (Buffer just fits)
mbedtls_mpi_write_binary:16:"123123123123123123123123":"012312312312312312312312312":14:0

Test mbedtls_mpi_write_binary #2 (Buffer too small)
mbedtls_mpi_write_binary:16:"123123123123123123123123":"123123123123123123123123":13:MBEDTLS_ERR_MPI_BUFFER_TOO_SMALL

Base test mbedtls_mpi_read_file #1
mbedtls_mpi_read_file:10:"data_files/mpi_10":"01f55332c3a48b910f9942f6c914e58bef37a47ee45cb164a5b6b8d1006bf59a059c21449939ebebfdf517d2e1dbac88010d7b1f141e997bd6801ddaec9d05910f4f2de2b2c4d714e2c14a72fc7f17aa428d59c531627f09":0

Test mbedtls_mpi_read_file #1 (Empty file)
mbedtls_mpi_read_file:10:"data_files/hash_file_4":"":MBEDTLS_ERR_MPI_FILE_IO_ERROR

Test mbedtls_mpi_read_file #2 (Illegal input)
mbedtls_mpi_read_file:10:"data_files/hash_file_3":"":0

Test mbedtls_mpi_read_file #3 (Input too big)
mbedtls_mpi_read_file:10:"data_files/mpi_too_big":"":MBEDTLS_ERR_MPI_BUFFER_TOO_SMALL

Base
test mbedtls_mpi_write_file #1
mbedtls_mpi_write_file:10:"561256809817522823341418963203724894906139636935563925208160178921113506041116976827054983195120490405166988278292920768080069408739749795845270734810126360163539134623767555567200198311873649935879019527573078308965316787277179 24":16:"data_files/mpi_write"

Base test mbedtls_mpi_lsb #1

mbedtls_mpi_lsb:10:"561256809817522823341418963203724894906139636935563925208160178921113506041
116976827054983195120490405166988278292920768080069408739749795845270734810126360163539134623
767555567200198311873649935879019527573078308965316787277179 24":2

Base test mbedtls_mpi_lsb #2
mbedtls_mpi_lsb:10:"24":3

Base test mbedtls_mpi_lsb #3
mbedtls_mpi_lsb:16:"24":2

Base test mbedtls_mpi_lsb #4
mbedtls_mpi_lsb:16:"2000":13

Base test mbedtls_mpi_bitlen #1
mbedtls_mpi_bitlen:10:"561256809817522823341418963203724894906139636935563925208160178921113506 0
411169768270549831951204904051669882782929207680800694087397497958452707348101263601635391346
237675555672001983118736499358790195275730783089653167872771792 4":764

Base
test mbedtls_mpi_bitlen #2
mbedtls_mpi_bitlen:10:"24":5

Base test mbedtls_mpi_bitlen #3
mbedtls_mpi_bitlen:10:"1":1

Base test mbedtls_mpi_bitlen #4
mbedtls_mpi_bitlen:10:"15":4

Base test mbedtls_mpi_bitlen #5
mbedtls_mpi_bitlen:10:"16":5

Base test mbedtls_mpi_bitlen #6
mbedtls_mpi_bitlen:10:"10":4

Base test mbedtls_mpi_bitlen #7
mbedtls_mpi_bitlen:10:"0":0

Base test mbedtls_mpi_cmp_int #1
mbedtls_mpi_cmp_int:693:693:0

Base test mbedtls_mpi_cmp_int #2
mbedtls_mpi_cmp_int:693:692:1

Base test mbedtls_mpi_cmp_int #3
mbedtls_mpi_cmp_int:693:694:-1

Base test mbedtls_mpi_cmp_int (Negative values) #1
mbedtls_mpi_cmp_int:-2:-2:0

Base test mbedtls_mpi_cmp_int (Negative values) #2
mbedtls_mpi_cmp_int:-2:-3:1

Base test mbedtls_mpi_cmp_int (Negative values) #3
mbedtls_mpi_cmp_int:-2:-1:-1

Base test mbedtls_mpi_cmp_mpi #1
mbedtls_mpi_cmp_mpi:10:"693":10:"693":0

Base
test mbedtls_mpi_cmp_mpi #2
mbedtls_mpi_cmp_mpi:10:"693":10:"692":1

Base test mbedtls_mpi_cmp_mpi #3
mbedtls_mpi_cmp_mpi:10:"693":10:"694":-1

Base test mbedtls_mpi_cmp_mpi (Negative values) #1
mbedtls_mpi_cmp_mpi:10:"-2":10:"-2":0

Base test mbedtls_mpi_cmp_mpi (Negative values) #2
mbedtls_mpi_cmp_mpi:10:"-2":10:"-3":1

Base test mbedtls_mpi_cmp_mpi (Negative values) #3
mbedtls_mpi_cmp_mpi:10:"-2":10:"-1":-1

Base test mbedtls_mpi_cmp_mpi (Mixed values) #4
mbedtls_mpi_cmp_mpi:10:"-3":10:"2":-1

Base test mbedtls_mpi_cmp_mpi (Mixed values) #5
mbedtls_mpi_cmp_mpi:10:"2":10:"-3":1

Base test mbedtls_mpi_cmp_mpi (Mixed values) #6
mbedtls_mpi_cmp_mpi:10:"-2":10:"31231231289798":-1

Base test mbedtls_mpi_cmp_abs #1
mbedtls_mpi_cmp_abs:10:"693":10:"693":0

Base test mbedtls_mpi_cmp_abs #2
mbedtls_mpi_cmp_abs:10:"693":10:"692":1

Base test mbedtls_mpi_cmp_abs #3
mbedtls_mpi_cmp_abs:10:"693":10:"694":-1

Base test mbedtls_mpi_cmp_abs (Negative values) #1
mbedtls_mpi_cmp_abs:10:"-2":10:"-2":0

Base

test mbedtls_mpi_cmp_abs (Negative values) #2
mbedtls_mpi_cmp_abs:10:"-2":10:"-3":-1

Base test mbedtls_mpi_cmp_abs (Negative values) #3
mbedtls_mpi_cmp_abs:10:"-2":10:"-1":1

Base test mbedtls_mpi_cmp_abs (Zero and Zero) #4
mbedtls_mpi_cmp_abs:10:"0":10:"0":0

Base test mbedtls_mpi_cmp_abs (Mix values) #1
mbedtls_mpi_cmp_abs:10:"-2":10:"2":0

Base test mbedtls_mpi_cmp_abs (Mix values) #2
mbedtls_mpi_cmp_abs:10:"2":10:"-3":-1

Base test mbedtls_mpi_cmp_abs (Mix values) #3
mbedtls_mpi_cmp_abs:10:"-2":10:"1":1

Base test mbedtls_mpi_copy #1
mbedtls_mpi_copy:0:1500

Base test mpi_copy_self #1
mpi_copy_self:14

Base test mbedtls_mpi_swap #1
mbedtls_mpi_swap:0:1500

Test mbedtls_mpi_shrink #1
mbedtls_mpi_shrink:2:2:4:4

Test mbedtls_mpi_shrink #2
mbedtls_mpi_shrink:4:2:4:4

Test mbedtls_mpi_shrink #3
mbedtls_mpi_shrink:8:2:4:4

Test mbedtls_mpi_shrink #4
mbedtls_mpi_shrink:8:4:4:4

Test mbedtls_mpi_shrink #5
mbedtls_mpi_shrink:8:6:4:6

Test mbedtls_mpi_shrink #6
mbedtls_mpi_shrink:4:2:0:2

Test
mbedtls_mpi_shrink #7
mbedtls_mpi_shrink:4:1:0:1

Test mbedtls_mpi_shrink #8
mbedtls_mpi_shrink:4:0:0:1

Test mbedtls_mpi_safe_cond_assign #1
mbedtls_mpi_safe_cond_assign:+1:"01":+1:"02"

Test mbedtls_mpi_safe_cond_assign #2
mbedtls_mpi_safe_cond_assign:+1:"FF000000000000000001":+1:"02"

Test mbedtls_mpi_safe_cond_assign #3
mbedtls_mpi_safe_cond_assign:+1:"01":+1:"FF000000000000000002"

Test mbedtls_mpi_safe_cond_assign #4
mbedtls_mpi_safe_cond_assign:+1:"01":-1:"02"

Test mbedtls_mpi_safe_cond_assign #5
mbedtls_mpi_safe_cond_assign:-1:"01":+1:"02"

Test mbedtls_mpi_safe_cond_assign #6
mbedtls_mpi_safe_cond_assign:-1:"01":-1:"02"

Test mbedtls_mpi_safe_cond_swap #1
mbedtls_mpi_safe_cond_swap:+1:"01":+1:"02"

Test mbedtls_mpi_safe_cond_swap #2
mbedtls_mpi_safe_cond_swap:+1:"FF000000000000000001":+1:"02"

Test mbedtls_mpi_safe_cond_swap #3
mbedtls_mpi_safe_cond_swap:+1:"01":+1:"FF000000000000000002"

Test mbedtls_mpi_safe_cond_swap #4
mbedtls_mpi_safe_cond_swap:+1:"01":-1:"02"

Test
mbedtls_mpi_safe_cond_swap #5
mbedtls_mpi_safe_cond_swap:-1:"01":+1:"02"

Test mbedtls_mpi_safe_cond_swap #6
mbedtls_mpi_safe_cond_swap:-1:"01":-1:"02"

Base test mbedtls_mpi_add_abs #1
mbedtls_mpi_add_abs:10:"12345678":10:"642531":10:"12988209"

Base test mbedtls_mpi_add_abs #2
mbedtls_mpi_add_abs:10:"-12345678":10:"642531":10:"12988209"

Base test mbedtls_mpi_add_abs #3

mbedtls_mpi_add_abs:10:"12345678":10:"-642531":10:"12988209"

Base test mbedtls_mpi_add_abs #4
mbedtls_mpi_add_abs:10:"-12345678":10:"-642531":10:"12988209"

Test mbedtls_mpi_add_abs #1
mbedtls_mpi_add_abs:10:"-
643808006803554439230129854961492699151386107534013432918073439524138264842370630061369715394
739134090922937332590384720397133335969549256322620979036686633213903952966175107096769180017
646161851573147596390153":10:"561256809817522823334980883135689350513838338385948998216646317845773371711936242431813600546696784104553291124345529427170840035413845948641299401450430867600312924833400689235061158782211898864911327727396616690449585311313277 71":10:"561256809817522823341418963203724894906139636935563925208160178921113506041116976827054983195120490405166988278292920768080069408739749795845270734810126360163539134623767555567200198311873649935879019527573078308965316787277179 24"

Test
mbedtls_mpi_add_abs #2 (add to first value)
mpi_add_abs_add_first:10:"123123":10:"123123":10:"246246"

Test mbedtls_mpi_add_abs #3 (add to second value)
mpi_add_abs_add_second:10:"123123":10:"123123":10:"246246"

Regression mbedtls_mpi_add_abs (add small to very large MPI with carry rollover)
mbedtls_mpi_add_abs:16:"FFFFFFFFFFFFFFFFFFFFFFFFFFFFF8":16:"08":16:"100000000000000000000000000000000"

Regression mbedtls_mpi_add_abs (add small to very large MPI with carry rollover)
mbedtls_mpi_add_abs:16:"08":16:"FFFFFFFFFFFFFFFFFFFFFFFFFFFFF8":16:"100000000000000000000000000000000"

Base test mbedtls_mpi_add_mpi #1
mbedtls_mpi_add_mpi:10:"12345678":10:"642531":10:"12988209"

Base test mbedtls_mpi_add_mpi
#2
mbedtls_mpi_add_mpi:10:"-12345678":10:"642531":10:"-11703147"

Base test mbedtls_mpi_add_mpi #3
mbedtls_mpi_add_mpi:10:"12345678":10:"-642531":10:"11703147"

Base test mbedtls_mpi_add_mpi #4
mbedtls_mpi_add_mpi:10:"-12345678":10:"-642531":10:"-12988209"

Test mbedtls_mpi_add_mpi #1
mbedtls_mpi_add_mpi:10:"203956878356401977405765866929034577280193993314348263094772646453283062722701277632936616063144088173312372882677123879538709400158306567338328279154499698366071906766440037074217117805690872792848149112022286332144876183376326512083574821647933992961249 91

731983621930427428024380310401500056379012 3":10:"5318722890542041841850847343751333994083036139821308566452994649309521786060458488771291478203879964281755642282047858461412075324629363398341394124019753387057946465954873243651947928221894730922739935805879645716596780844841526038810941769955948133022842320060017521281689012935600518336468814362 19":10:"7358291674106061615908506013041679766884976072964791197400721113842352413287471265100657638835320846014879371108819097256799169326212429071724676915564750370718665533619273614394119106278803458851221426926102509038045542678604791159646689986435288062635341493258379714324431815373631558486474452263342"

Test mbedtls_mpi_add_mpi #2
mbedtls_mpi_add_mpi:10:"643808006803554439230129854961492699151386107534013432918073439524138264842370630061369715394739134090922937332590384720397133335969549256322620979036686633213903952966175107096769180017646161851573147596390153":10:"561256809817522823334980883135689350513838338385948998216646317845773371711936242431813600546696784104553291124345529427170840035413845948641299401450430867600312924833400689235061158782211898864911327727396616690449585311313277 71":10:"561256809817522823341418963203724894906139636935563925208160178921113506041116976827054983195120490405166988278292920768080069408739749795845270734810126360163539134623767555567200198311873649935879019527573078308965316787277179 24"

Base test mbedtls_mpi_add_mpi inplace #1
mbedtls_mpi_add_mpi_inplace:10:"12345678":10:"24691356"

Test mbedtls_mpi_add_mpi inplace #2
mbedtls_mpi_add_mpi_inplace:10:"643808006803554439230129854961492699151386107534013432918073439524138264842370630061369715394739134090922937332590384720397133335969549256322620979036686633213903952966175107096769180017646161851573147596390153":10:"128761601360710887846025970992298539830277221506802686583614687904827652968474126012273943078947826818184587466518076944079426667193909851264524195807337326642780790593235021419353836003529232370314629519278030 6"

Test mbedtls_mpi_add_mpi inplace #3
mbedtls_mpi_add_mpi_inplace:16:"ffffffffffffffffffffffffffffffff":16:"01fffffffffffffffffffffffffffffe"

Test mbedtls_mpi_add_int #1
mbedtls_mpi_add_int:10:"203956878356401977405765866929034577280193993314348263094772646453283062 7227012776329":9871232:10:"203956878356401977405765866929034577280193993314348263094772646453283062627227022647561"

Test mbedtls_mpi_add_int #2
mbedtls_mpi_add_int:10:"203956878356401977405765866929034577280193993314348263094772646453283062 7227012776329":-9871232:10:"203956878356401977405765866929034577280193993314348263094772646453283062722702290509 7"

Base test mbedtls_mpi_sub_abs #1 (Test with larger second input)
mbedtls_mpi_sub_abs:10:"5":10:"7":10:"0":MBEDTLS_ERR_MPI_NEGATIVE_VALUE

Base test mbedtls_mpi_sub_abs #2 (Test with larger second input)
mbedtls_mpi_sub_abs:10:"-5":10:"-7":10:"0":MBEDTLS_ERR_MPI_NEGATIVE_VALUE

Base test mbedtls_mpi_sub_abs #3 (Test with larger second input)
mbedtls_mpi_sub_abs:10:"-5":10:"7":10:"0":MBEDTLS_ERR_MPI_NEGATIVE_VALUE

Base test mbedtls_mpi_sub_abs #4 (Test with larger second input)
mbedtls_mpi_sub_abs:10:"5":10:"-7":10:"0":MBEDTLS_ERR_MPI_NEGATIVE_VALUE

Base test mbedtls_mpi_sub_abs #1
mbedtls_mpi_sub_abs:10:"7":10:"5":10:"2":0

Base test mbedtls_mpi_sub_abs #2
mbedtls_mpi_sub_abs:10:"-7":10:"-5":10:"2":0

Base test mbedtls_mpi_sub_abs #3
mbedtls_mpi_sub_abs:10:"-7":10:"5":10:"2":0

Base test mbedtls_mpi_sub_abs
#4
mbedtls_mpi_sub_abs:10:"7":10:"-5":10:"2":0

Test mbedtls_mpi_sub_abs #1
mbedtls_mpi_sub_abs:16:"FFFFFFFFFF":16:"01":16:"FFFFFFFFFE":0

Test mbedtls_mpi_sub_abs #2
mbedtls_mpi_sub_abs:16:"FFFFFFFFF0":16:"01":16:"FFFFFFFFEF":0

Test mbedtls_mpi_sub_abs #3
mbedtls_mpi_sub_abs:16:"FF00000000":16:"0F00000000":16:"F000000000":0

Test mbedtls_mpi_sub_abs #4
mbedtls_mpi_sub_abs:16:"FF00000000":16:"0F00000001":16:"EFFFFFFFFF":0

Base test mbedtls_mpi_sub_mpi #1 (Test with negative result)
mbedtls_mpi_sub_mpi:10:"5":10:"7":10:"-2"

Base test mbedtls_mpi_sub_mpi #2 (Test with negative inputs)
mbedtls_mpi_sub_mpi:10:"-5":10:"-7":10:"2"

Base test mbedtls_mpi_sub_mpi #3 (Test with negative base)
mbedtls_mpi_sub_mpi:10:"-5":10:"7":10:"-12"

Base test mbedtls_mpi_sub_mpi #4 (Test with negative subtraction)
mbedtls_mpi_sub_mpi:10:"5":10:"-7":10:"12"

Test mbedtls_mpi_sub_mpi #1

mbedtls_mpi_sub_mpi:10:"53187228905420418418508473437513339940830361398213085664529946493095217
86060458488771291478203879964281755642282047858461412075324629363398341394124019753387057946465954873243651947928221894730922739935805879645716596780844841526038810941769955948133022842320060017521281689012935600518336468814362 19":10:"20395687835640197740576586692903457728019399331434826309477264645328306272270226475614 31434826309477264645328306272270127763293661606314408817331237288267712387953870940015830656733832827915449969836607190676644003707421711780569087279284814911202228633214487618337632651208357482164793399296124991731983621930427428024380310401500056379012 3":10:"3279154106978022067793188674460988221281096206677825935505268184776691158833445712441925317572439082548631913455276619666024981323046297724958111332474756403397227398290472872909776750164986002994258444685656782395148019011078260917975193553476608203410343146861655328238946210497569478186463176460 96"

Test
 mbedtls_mpi_sub_mpi #2 (Test for negative result)
mbedtls_mpi_sub_mpi:10:"643808006803554439230129854961492699151386107534013432918073439524138264842370630061369715394739134090922937332590384720397133335969549256322620979036686633213903952966175107096769180017646161851573147596390153":10:"561256809817522823334980883135689350513838338385948998216646317845773371711936242431813600546696784104553291124345529427170840035413845948641299401450430867600312924833400689235061158782211898864911327727396616690449585311313277 71":10:"-561256809817522823328542803067653806121537039836334071225132456770433237382755508036572217898273077803939593970398138086261610662087942101437328068090735375037086715043033822902922119252550147793943635927220155071933853835349376 18"

Test
 mbedtls_mpi_sub_int #1
mbedtls_mpi_sub_int:10:"203956878356401977405765866929034577280193993314348263094772646453283062 7227012776329":-9871232:10:"203956878356401977405765866929034577280193993314348263094772646453283062722701277632 9561"

Test mbedtls_mpi_sub_int #2
mbedtls_mpi_sub_int:10:"203956878356401977405765866929034577280193993314348263094772646453283062 7227012776329":9871232:10:"203956878356401977405765866929034577280193993314348263094772646453283062722700290509 7"

Test
 mbedtls_mpi_shift_l #1
mbedtls_mpi_shift_l:10:"64":1:10:"128"

Test mbedtls_mpi_shift_l #2
mbedtls_mpi_shift_l:10:"658385546911733550164516088405238961461880256029834598831972039469421755117818013653494814438931957316403111689187691446941406788869098983929874080332195117465344344350008880118042764943201875870917468833709791733282363323948005998269792207":37:10:"904878205486390206919223046197230763054009616101198848727231906786428041683823678566861345318656430669830172498462864502512723643656050227509004394375953550529450359155792165573305054387349553405261454769882501711814049667182892597433788836409811927 04"

Test mbedtls_mpi_shift_r #1
mbedtls_mpi_shift_r:10:"128":1:10:"64"

Test mbedtls_mpi_shift_r #2
mbedtls_mpi_shift_r:10:"120815570979701484704906977000760567182871429114712069861589084706550626575967516787438008593490722779337547394120718248995900363209947025063336882559539208430319216688889117222633155838468458047056355241515415159736436403445579777425189969":45:10:"343378505305342641534329507637609615309405140563717594266077767049837992135415779521957826413798564940798165122602990348343326909372157800428729167832498229786094773001221702834962899937830963060197164058750488378951889681745 7"

Test
mbedtls_mpi_shift_r #4
mbedtls_mpi_shift_r:16:"FFFFFFFFFFFFFFFF":63:16:"01"

Test mbedtls_mpi_shift_r #4
mbedtls_mpi_shift_r:16:"FFFFFFFFFFFFFFFF":64:16:"00"

Test mbedtls_mpi_shift_r #6
mbedtls_mpi_shift_r:16:"FFFFFFFFFFFFFFFF":65:16:"00"

Test mbedtls_mpi_shift_r #7
mbedtls_mpi_shift_r:16:"FFFFFFFFFFFFFFFF":128:16:"00"

Base test mbedtls_mpi_mul_mpi #1
mbedtls_mpi_mul_mpi:10:"5":10:"7":10:"35"

Base test mbedtls_mpi_mul_mpi #2
mbedtls_mpi_mul_mpi:10:"-5":10:"7":10:"-35"

Base test mbedtls_mpi_mul_mpi #3
mbedtls_mpi_mul_mpi:10:"5":10:"-7":10:"-35"

Base test mbedtls_mpi_mul_mpi #4
mbedtls_mpi_mul_mpi:10:"-5":10:"-7":10:"35"

Test mbedtls_mpi_mul_mpi #1
mbedtls_mpi_mul_mpi:10:"2891171001732020596616782072531323436153525916304586798627747814508107684584649352134869325353001124398816014806342483789597194824416786723692391950696231218582991448299347894765747235146133672964148506932363542469293027888892345006054646588349094426514785103681743397098474773302052225953 7":10:"164715818917017947647040097190573499962702399489934522688129750372405860999247127153669674865874178037539163343313555737769452388715120268328106262261643463288074076693660299262214153835608143388284496422653778227597680114067570610635247681405678673502085544393423204105513416751190780509 53":10:"476221599179424887669515829231223263939342135681791605842540429321038144633323941248706405375723482912535192363845116154236465184147599697841273424891410002781967962186252583311115708128167171262206919514587899883547279647025952837516324649656913580411611297312678955801899536937577476819667861053063432906071315727948826276092545739432005962781562403795455162483159362585281248265005441715080197800335757871588

045959754547836825977169125866324128449699877076762316768127816074587766799018626179199776188490087103869164122906791440101822594139648973454716256383294690817576188761"

Test
mbedtls_mpi_mul_int #1
mbedtls_mpi_mul_int:10:"203956878356401977405765866929034577280193993314348263094772646453283062722701277632 9":9871232:10:"201330566425182260423107301013762784835472391301238063380553878039433427380633597821076673328":":=="

Test mbedtls_mpi_mul_int #2 (Unsigned, thus failure)
mbedtls_mpi_mul_int:10:"203956878356401977405765866929034577280193993314348263094772646453283062722701277632 9":-9871232:10:"-201330566425182260423107301013762784835472391301238063380553878039433427380633597821076673328":"!="

Test mbedtls_mpi_mul_int #3
mbedtls_mpi_mul_int:10:"-203956878356401977405765866929034577280193993314348263094772646453283062722701277632 9":9871232:10:"-201330566425182260423107301013762784835472391301238063380553878039433427380633597821076673328":"=="

Test mbedtls_mpi_mul_int #4 (Unsigned, thus failure)
mbedtls_mpi_mul_int:10:"-203956878356401977405765866929034577280193993314348263094772646453283062722701277632 9":-9871232:10:"201330566425182260423107301013762784835472391301238063380553878039433427380633597821076673328":"!="

Base
test mbedtls_mpi_div_mpi #1
mbedtls_mpi_div_mpi:10:"1000":10:"13":10:"76":10:"12":0

Base test mbedtls_mpi_div_mpi #2 (Divide by zero)
mbedtls_mpi_div_mpi:10:"1000":10:"0":10:"1":10:"1":MBEDTLS_ERR_MPI_DIVISION_BY_ZERO

Base test mbedtls_mpi_div_mpi #3
mbedtls_mpi_div_mpi:10:"1000":10:"-13":10:"-76":10:"12":0

Test mbedtls_mpi_div_mpi #1
mbedtls_mpi_div_mpi:10:"201330566425182260423107301013762784835472391301238063380553878039433427380633597821076673328":10:"34":10:"592148724779947824773845002981655249516095268533053127589864347174804198178334111238460803":10:"26":0

Test mbedtls_mpi_div_mpi #2
mbedtls_mpi_div_mpi:10:"476221599179424887669515829231223263939342135681791605842540429321038144633323941248706405375723482912535192363845116154236465184147599697841273424891410002781967962186252583311115708128167171262206919514587899883547279647025952837516324649656913580411611297312678955801899536937577476819667861053063432906071315727948826276092545739432005962781562 40

37954551624831593625852812482650054417150801978003357578715880459597545478368259771691258663241284496998770767623167681278160745877667990186261791997761884900871038691641229067914401018225941396489734547162563832946908175761887621:10:"289117100173202059661678207253132343615352591630458679862774781450810768458464935213486932535300112439881601480634248378959719482441678672369239195069623121858299144829934789476574723514613367296414850693236354246929302788889234500605464658834909442651478510368174339709847477330205222595371:10:"164715818917017947647040097190573499962702399489934522688129750372405860999247127153669674865874178037539163343313555737769452388715120268328106262261643463288074076693660299262214153835608143388284496422653778227597680114067570610635247681405678673502085544393423204105513416751190780509531:10:"1":0

Test
 mbedtls_mpi_div_mpi #3
mbedtls_mpi_div_mpi:10:"1000":10:"7":10:"142":10:"6":0

Test mbedtls_mpi_div_mpi #4
mbedtls_mpi_div_mpi:10:"777":10:"7":10:"111":10:"0":0

Base test mbedtls_mpi_div_int #1
mbedtls_mpi_div_int:10:"1000":13:10:"76":10:"12":0

Base test mbedtls_mpi_div_int #2 (Divide by zero)
mbedtls_mpi_div_int:10:"1000":0:10:"1":10:"1":MBEDTLS_ERR_MPI_DIVISION_BY_ZERO

Base test mbedtls_mpi_div_int #3
mbedtls_mpi_div_int:10:"1000":-13:10:"-76":10:"12":0

Test mbedtls_mpi_div_int #1
mbedtls_mpi_div_int:10:"2013305664251822604231073010137627848354723913012380633805538780394334273806335978210766732 8":34:10:"5921487247799478247738450029816552495160952685330531275898643471748041981783341112384608 03":10:"26":0

Test mbedtls_mpi_div_int #2
mbedtls_mpi_div_int:10:"2013305664251822604231073010137627848354723913012380633805538780394334273806335978210766732 8":-34:10:"-5921487247799478247738450029816552495160952685330531275898643471748041981783341112384608 03":10:"26":0

Base
 test mbedtls_mpi_mod_mpi #1
mbedtls_mpi_mod_mpi:10:"1000":10:"13":10:"12":0

Base test mbedtls_mpi_mod_mpi #2 (Divide by zero)
mbedtls_mpi_mod_mpi:10:"1000":10:"0":10:"0":MBEDTLS_ERR_MPI_DIVISION_BY_ZERO

Base test mbedtls_mpi_mod_mpi #3
mbedtls_mpi_mod_mpi:10:"-1000":10:"13":10:"1":0

Base test mbedtls_mpi_mod_mpi #4 (Negative modulo)

mbedtls_mpi_mod_mpi:10:"1000":10:"-13":10:"-1":MBEDTLS_ERR_MPI_NEGATIVE_VALUE

Base test mbedtls_mpi_mod_mpi #5 (Negative modulo)
mbedtls_mpi_mod_mpi:10:"-1000":10:"-13":10:"-12":MBEDTLS_ERR_MPI_NEGATIVE_VALUE

Base test mbedtls_mpi_mod_int #1
mbedtls_mpi_mod_int:10:"1000":13:12:0

Base test mbedtls_mpi_mod_int #2 (Divide by zero)
mbedtls_mpi_mod_int:10:"1000":0:0:MBEDTLS_ERR_MPI_DIVISION_BY_ZERO

Base test mbedtls_mpi_mod_int #3
mbedtls_mpi_mod_int:10:"-1000":13:1:0

Base test mbedtls_mpi_mod_int #4 (Negative modulo)
mbedtls_mpi_mod_int:10:"1000":-13:0:MBEDTLS_ERR_MPI_NEGATIVE_VALUE

Base test mbedtls_mpi_mod_int #5 (Negative modulo)
mbedtls_mpi_mod_int:10:"-1000":-13:0:MBEDTLS_ERR_MPI_NEGATIVE_VALUE

Base
 test mbedtls_mpi_mod_int #6 (By 1)
mbedtls_mpi_mod_int:10:"1000":1:0:0

Base test mbedtls_mpi_mod_int #7 (By 2)
mbedtls_mpi_mod_int:10:"1001":2:1:0

Base test mbedtls_mpi_mod_int #8 (By 2)
mbedtls_mpi_mod_int:10:"1000":2:0:0

Base test mbedtls_mpi_exp_mod #1
mbedtls_mpi_exp_mod:10:"23":10:"13":10:"29":10:"":10:"24":0

Base test mbedtls_mpi_exp_mod #2 (Even N)
mbedtls_mpi_exp_mod:10:"23":10:"13":10:"30":10:"":10:"0":MBEDTLS_ERR_MPI_BAD_INPUT_DATA

Base test mbedtls_mpi_exp_mod #3 (Negative N)
mbedtls_mpi_exp_mod:10:"23":10:"13":10:"-29":10:"":10:"0":MBEDTLS_ERR_MPI_BAD_INPUT_DATA

Base test mbedtls_mpi_exp_mod #4 (Negative base)
mbedtls_mpi_exp_mod:10:"-23":10:"13":10:"29":10:"":10:"5":0

Base test mbedtls_mpi_exp_mod #5 (Negative exponent)
mbedtls_mpi_exp_mod:10:"23":10:"-13":10:"29":10:"":10:"0":MBEDTLS_ERR_MPI_BAD_INPUT_DATA

Base test mbedtls_mpi_exp_mod #7 (Negative base + exponent)
mbedtls_mpi_exp_mod:10:"-23":10:"-13":10:"29":10:"":10:"0":MBEDTLS_ERR_MPI_BAD_INPUT_DATA

Test
mbedtls_mpi_exp_mod #1
mbedtls_mpi_exp_mod:10:"433019240910377478217373572959560109819648647016096560523769010881172869083338285573756574557395862965095016483867813043663981946477698466501451832407592327356331263124555137732393938242285782144928753919588632679050799198937132922145084847":10:"57815383279778288971509091667784076592504583796458230620424924615767585267574909100736280086139775505463827747755708881300297635715286995747175832289395359602344642308825736159303849791003791029156574838667553715598117187677605949194569713541841137 21":10:"583137007797276923956891216216022144052044091311388601652961409557516421612874571554415606746479105795833145583959622117418531166391184939066520869800857530421873250114773204354963864729386957427276448683092491947566992077136553066273207777134303397724679138833126700957":10:"":10:"1145974492766843551449206700071479532326594363801634615531869401139297771960181641497035664729365788909910493444592041998882549071134957947304526998422739395810481420048343303694838138766187725788690832480616164443920916937870396363168455122921270978650262901730048607 36":0

Test
mbedtls_mpi_exp_mod (Negative base)
mbedtls_mpi_exp_mod:10:"-10000000000":10:"10000000000":10:"99999":10:"":10:"1":0

Test mbedtls_mpi_exp_mod (Negative base)
mbedtls_mpi_exp_mod:16:"-9f13012cd92aa72fb86ac8879d2fde4f7fd661aaae43a00971f081cc60ca277059d5c37e89652e2af2585d281d66ef6a9d38a117e9608e9e7574cd142dc55278838a2161dd56db9470d4c1da2d5df15a908ee2eb886aaa890f23be16de59386663a12f1afbb325431a3e835e3fd89b98b96a6f77382f458ef9a37e1f84a03045c8676ab55291a94c2228ea15448ee96b626b998":16:"40a54d1b9e86789f06d9607fb158672d64867665c73ee9abb545fc7a785634b354c7bae5b962ce8040cf45f2c1f3d3659b2ee5ede17534c8fc2ec85c815e8df1fe7048d12c90ee31b88a68a081f17f0d8ce5f4030521e9400083bcea73a429031d4ca7949c2000d597088e0c39a6014d8bf962b73bb2e8083bd0390a4e00b9b3":16:"eeaf0ab9adb38dd69c33f80afa8fc5e86072618775ff3c0b9ea2314c9c256576d674df7496ea81d3383b4813d692c6e0e0d5d8e250b98be48e495c1d6089dad15dc7d7b46154d6b6ce8ef4ad69b15d4982559b297bcf1885c529f566660e57ec68edbc3c05726cc02fd4cbf4976eaa9afd5138fe8376435b9fc61d2fc0eb06e3":16:"":16:"21acc7199e1b90f9b4844ffe12c19f00ec548c5d32b21c647d48b6015d8eb9ec9db05b4f3d44db4227a2b5659c1a7cceb9d5fa8fa60376047953ce7397d90aaeb7465e14e820734f84aa52ad0fc66701bcbb991d57715806a11531268e1e83dd48288c72b424a6287e9ce4e5cc4db0dd67614aecc23b0124a5776d36e5c89483":0

Base
test GCD #1
mbedtls_mpi_gcd:10:"693":10:"609":10:"21"

Base test GCD #2
mbedtls_mpi_gcd:10:"1764":10:"868":10:"28"

Base test GCD #3
mbedtls_mpi_gcd:10:"768454923":10:"542167814":10:"1"

Test GCD #1
mbedtls_mpi_gcd:10:"433019240910377478217373572959560109819648647016096560523769010881172869083338285573756574557395862965095016483867813043663981946477698466501451832407592327356331263124555137732393938242285782144928753919588632679050799198937132922145084847":10:"5781538327977828

897150909166778407659250458379645823062042492461576758526757490910073628008613977550546382774
775570888130029763571528699574717583228939535960234464230882573615930384979100379102915657483
866755371559811718767760594919456971354184113721":10:"1"

Base
test mbedtls_mpi_inv_mod #1
mbedtls_mpi_inv_mod:10:"3":10:"11":10:"4":0

Base test mbedtls_mpi_inv_mod #2
mbedtls_mpi_inv_mod:10:"3":10:"0":10:"0":MBEDTLS_ERR_MPI_BAD_INPUT_DATA

Base test mbedtls_mpi_inv_mod #3
mbedtls_mpi_inv_mod:10:"3":10:"-11":10:"4":MBEDTLS_ERR_MPI_BAD_INPUT_DATA

Base test mbedtls_mpi_inv_mod #4
mbedtls_mpi_inv_mod:10:"2":10:"4":10:"0":MBEDTLS_ERR_MPI_NOT_ACCEPTABLE

Base test mbedtls_mpi_inv_mod #5
mbedtls_mpi_inv_mod:10:"3":10:"1":10:"0":MBEDTLS_ERR_MPI_BAD_INPUT_DATA

Test mbedtls_mpi_inv_mod #1
mbedtls_mpi_inv_mod:16:"aa4df5cb14b4c31237f98bd1faf527c283c2d0f3eec89718664ba33f9762907c":16:"fffbbd
660b94412ae61ead9c2906a344116e316a256fd387874c6c675b1d587d":16:"8d6a5c1d7adeae3e94b9bcd2c47e0d46e
778bc8804a2cc25c02d775dc3d05b0c":0

Base test mbedtls_mpi_is_prime #1
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_is_prime:10:"0":MBEDTLS_ERR_MPI_NOT_ACCEPTABLE

Base
test mbedtls_mpi_is_prime #2
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_is_prime:10:"1":MBEDTLS_ERR_MPI_NOT_ACCEPTABLE

Base test mbedtls_mpi_is_prime #3
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_is_prime:10:"2":0

Base test mbedtls_mpi_is_prime #4
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_is_prime:10:"3":0

Base test mbedtls_mpi_is_prime #5
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_is_prime:10:"4":MBEDTLS_ERR_MPI_NOT_ACCEPTABLE

Base test mbedtls_mpi_is_prime #6
depends_on:MBEDTLS_GENPRIME

mbedtls_mpi_is_prime:10:"5":0

Base test mbedtls_mpi_is_prime #7
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_is_prime:10:"27":MBEDTLS_ERR_MPI_NOT_ACCEPTABLE

Base test mbedtls_mpi_is_prime #8
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_is_prime:10:"47":0

Test mbedtls_mpi_is_prime #1a
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_is_prime:10:"837267288831461519796682433260970492892084829876859652764391571623374764
77581":MBEDTLS_ERR_MPI_NOT_ACCEPTABLE

Test
mbedtls_mpi_is_prime #1b
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_is_prime:10:"8124863741058492145486930848889926709653064363273025820125609258228126324
4641":MBEDTLS_ERR_MPI_NOT_ACCEPTABLE

Test mbedtls_mpi_is_prime #2a
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_is_prime:10:"827131507221654563937832686696200995595835694437983658840870036586124168
186967796809117749047430768825822857042432722828096779098498192459819306321073968735177531164
565305635281198148032612029767584644305912099":0

Test mbedtls_mpi_is_prime #2b
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_is_prime:10:"827131507221654563937832686696200995595835694437983658840870036586124168
186967796809117749047430768825822857042432722828096779098498192459819306321073968735177531164
565305635281198148032612029767584644305912001":MBEDTLS_ERR_MPI_NOT_ACCEPTABLE

Test mbedtls_mpi_is_prime #3
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_is_prime:10:"2833419889721787128217599":0

Test mbedtls_mpi_is_prime #4
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_is_prime:10:"195845982777569926302400511":0

Test
mbedtls_mpi_is_prime #5
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_is_prime:10:"4776913109852041418248056622882488319":0

Test mbedtls_mpi_is_prime #5
depends_on:MBEDTLS_GENPRIME

mbedtls_mpi_is_prime:10:"768614336404564651":0

Test mbedtls_mpi_is_prime #6
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_is_prime:10:"201487636602438195784363":0

Test mbedtls_mpi_is_prime #7
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_is_prime:10:"845100400152152934331135470251":0

Test mbedtls_mpi_is_prime #8
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_is_prime:10:"5671372782015641057722910123862803524 3":0

Test mbedtls_mpi_is_prime #9
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_is_prime:10:"203956878356401977405765866929034577280193993314348263094772646453283062722701277632936616063144088173312372882677123879538709400158306567338328279154499698366071906766440037074217117805690872792848149112022286332144876183376326512083574821647933992961249917319836219304274280243803104015000563790123":0

Test
mbedtls_mpi_is_prime #10
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_is_prime:10:"53187228905420418418508473437513339940830361398213085664529946493095217860604584887712914782038799642817556422820478584614120753246293633983413941240197533870579464659548732436519479282218947309227399358058796457165967808448415260388109417699559481330228423200600175212816890129356005183364688143621 9":0

Test mbedtls_mpi_is_prime #11
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_is_prime:10:"319705304701141539155720137200974664666792526059405792539680974929469783512821793995613718943171723765238853752439032835985158829038528214925658918372196742089464683960239919950882355844766055365179937610326127675178857306260955550407044463370239890187189750909036833976197804646589380690779463976173":0

Test mbedtls_mpi_is_prime #12
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_is_prime:10:"200603822195324642393516294012917598972967449320074999667103434371470616000652036570009912021332527788252300901905236578801044680456930305350440933538867383130165841118050781326291059830545891570648243241795871":0

Test
mbedtls_mpi_is_prime #13
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_is_prime:10:"827131507221654563937832686696200995595835694437983658840870036586124168186967796809117749047430768825822857042432722828096779098498192459819306321073968735177531164565305635281198148032612029767584644305912099":0

Test mbedtls_mpi_is_prime #14
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_is_prime:10:"964274047248418797145090983157197980855078966882276492572788532954904112655338439361306213898569516593744267391754033306465125919199692703323878557833023573312685002670662846477592597659826113460619815244721311":0

Test mbedtls_mpi_is_prime #15
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_is_prime:10:"170141183460469231731687303715884105727":0

Test mbedtls_mpi_is_prime #16
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_is_prime:10:"2147483647":0

Test mbedtls_mpi_is_prime #17
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_is_prime:10:"961748941":0

Test
mbedtls_mpi_is_prime #18
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_is_prime:10:"179424691":0

Test mbedtls_mpi_is_prime #19
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_is_prime:10:"32452867":0

Test mbedtls_mpi_is_prime #20
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_is_prime:10:"49979687":0

Test mbedtls_mpi_gen_prime (Too small)
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_gen_prime:2:0:MBEDTLS_ERR_MPI_BAD_INPUT_DATA

Test mbedtls_mpi_gen_prime (OK, minimum size)
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_gen_prime:3:0:0

Test mbedtls_mpi_gen_prime (Larger)
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_gen_prime:128:0:0

Test mbedtls_mpi_gen_prime (Safe)
depends_on:MBEDTLS_GENPRIME
mbedtls_mpi_gen_prime:128:1:0

Test bit getting (Value bit 25)
mbedtls_mpi_get_bit:10:"49979687":25:1

Test bit getting (Larger but same limb)
mbedtls_mpi_get_bit:10:"49979687":26:0

Test bit getting (Larger and non-existing limb)
mbedtls_mpi_get_bit:10:"49979687":500:0

Test bit getting (Value bit 24)
mbedtls_mpi_get_bit:10:"49979687":24:0

Test
bit getting (Value bit 23)
mbedtls_mpi_get_bit:10:"49979687":23:1

Test bit set (Change existing value with a 1)
mbedtls_mpi_set_bit:10:"49979687":24:1:10:"66756903":0

Test bit set (Change existing value with a 0)
mbedtls_mpi_set_bit:10:"49979687":25:0:10:"16425255":0

Test bit set (Add above existing limbs with a 0)
mbedtls_mpi_set_bit:10:"49979687":80:0:10:"49979687":0

Test bit set (Add above existing limbs with a 1)
mbedtls_mpi_set_bit:10:"49979687":80:1:10:"120892581961462922468586 3":0

Test bit set (Bit index larger than 31 with a 0)
mbedtls_mpi_set_bit:16:"FFFFFFFFFFFFFFFF":32:0:16:"FFFFFFFEFFFFFFFF":0

Test bit set (Bit index larger than 31 with a 1)
mbedtls_mpi_set_bit:16:"00":32:1:16:"0100000000":0

Test bit set (Invalid bit value)
mbedtls_mpi_set_bit:16:"00":5:2:16:"00":MBEDTLS_ERR_MPI_BAD_INPUT_DATA

MPI Selftest
depends_on:MBEDTLS_SELF_TEST
mpi_selftest:
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTYwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTcwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAARrISq2zO9m
D29YCLHB56FdU/RINtRhfeLtM+u5o3HaAnopy0S98RzuEGELjpzr8ZI6kkMMZsj8
nFZQF8HfuE0go4GJMIGGMB0GA1UdDgQWBBSnjWvpWxZcFnfQ2KGtCg/u6fT/DzBX
BgNVHSMEUDBOgBRTw3K0Psy3u/6+3KKSoaQqJnPvPqEzpDEwLzELMAkGA1UEBhMC

VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTE1ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgDgXjoc6FfMF5W0NziV6vx2BOPNWav01Z
ynEP4h9ULnUCIQC1rU4sEId3UdjzTKhpSGTKtaOuPG+b0YdEMPimI4jmVw==
-----END CERTIFICATE-----
-----BEGIN X509 CRL-----
MIIBqzCBlDANBgkqhkiG9w0BAQ4FADA7MQswCQYDVQQGEwJOTDERMA8GA1UEChMI
UG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EXDTExMDIxMjE0NDQw
N1oXDTExMDQxMzE0NDQwN1owKDASAgEBFw0xMTAyMTIxNDQ0MDdaMBICAQMXDTEx
MDIxMjE0NDQwN1owDQYJKoZIhvcNAQEOBQADggEBAL2sIly2OwgBu9UfEImduTG/
RtGEO8RkXbCRJPLZaVGQh9b8rCRVHL9tIWm372FVkKyYEm3mIrl2ry16RznRt5yx
Dd8/DKUGUlIe1KwzjDc9O7bv1FDSXHd1USmGTheKDHNtuJXYENMHdoyR2k2BVGOZ
ie4zUcSpqyMjBlUjgNmXN6gQIcrRImumVUjMk74+rWTa0hQ0piF2qlRuE1dDqcZP
LkE/92rbnFeRAO91XUeEj13dif2UjlArFWd62AFp0wtIn2sb7wahhUj9/rEs6Wgx
kdiNsRMto6/ixLrPu3vxs80ZPWHey587T1ZZ9bS/wDkp9W+W0rGyRoPVmqiKtvM=
-----END X509 CRL-----
ARC4 Encrypt and decrypt 0 bytes
depends_on:MBEDTLS_ARC4_C
enc_dec_buf:MBEDTLS_CIPHER_ARC4_128:"ARC4-128":128:0:-1

ARC4 Encrypt and decrypt 1 byte
depends_on:MBEDTLS_ARC4_C
enc_dec_buf:MBEDTLS_CIPHER_ARC4_128:"ARC4-128":128:1:-1

ARC4 Encrypt and decrypt 2 bytes
depends_on:MBEDTLS_ARC4_C
enc_dec_buf:MBEDTLS_CIPHER_ARC4_128:"ARC4-128":128:2:-1

ARC4 Encrypt and decrypt 7 bytes
depends_on:MBEDTLS_ARC4_C
enc_dec_buf:MBEDTLS_CIPHER_ARC4_128:"ARC4-128":128:7:-1

ARC4 Encrypt and decrypt 8 bytes
depends_on:MBEDTLS_ARC4_C
enc_dec_buf:MBEDTLS_CIPHER_ARC4_128:"ARC4-128":128:8:-1

ARC4 Encrypt and decrypt 9 bytes
depends_on:MBEDTLS_ARC4_C
enc_dec_buf:MBEDTLS_CIPHER_ARC4_128:"ARC4-128":128:9:-1

ARC4 Encrypt and decrypt 15 bytes
depends_on:MBEDTLS_ARC4_C
enc_dec_buf:MBEDTLS_CIPHER_ARC4_128:"ARC4-128":128:15:-1

ARC4 Encrypt and decrypt 16 bytes
depends_on:MBEDTLS_ARC4_C
enc_dec_buf:MBEDTLS_CIPHER_ARC4_128:"ARC4-128":128:16:-1

ARC4 Encrypt and decrypt 17 bytes

depends_on:MBEDTLS_ARC4_C
enc_dec_buf:MBEDTLS_CIPHER_ARC4_128:"ARC4-128":128:17:-1

ARC4
Encrypt and decrypt 31 bytes
depends_on:MBEDTLS_ARC4_C
enc_dec_buf:MBEDTLS_CIPHER_ARC4_128:"ARC4-128":128:31:-1

ARC4 Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_ARC4_C
enc_dec_buf:MBEDTLS_CIPHER_ARC4_128:"ARC4-128":128:32:-1

ARC4 Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_ARC4_C
enc_dec_buf:MBEDTLS_CIPHER_ARC4_128:"ARC4-128":128:33:-1

ARC4 Encrypt and decrypt 47 bytes
depends_on:MBEDTLS_ARC4_C
enc_dec_buf:MBEDTLS_CIPHER_ARC4_128:"ARC4-128":128:47:-1

ARC4 Encrypt and decrypt 48 bytes
depends_on:MBEDTLS_ARC4_C
enc_dec_buf:MBEDTLS_CIPHER_ARC4_128:"ARC4-128":128:48:-1

ARC4 Encrypt and decrypt 49 bytes
depends_on:MBEDTLS_ARC4_C
enc_dec_buf:MBEDTLS_CIPHER_ARC4_128:"ARC4-128":128:49:-1

ARC4 Encrypt and decrypt 0 bytes in multiple parts
depends_on:MBEDTLS_ARC4_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_ARC4_128:128:0:0:

ARC4 Encrypt and decrypt 1 bytes in multiple parts 1
depends_on:MBEDTLS_ARC4_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_ARC4_128:128:1:0:

ARC4
Encrypt and decrypt 1 bytes in multiple parts 2
depends_on:MBEDTLS_ARC4_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_ARC4_128:128:0:1:

ARC4 Encrypt and decrypt 16 bytes in multiple parts 1
depends_on:MBEDTLS_ARC4_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_ARC4_128:128:16:0:

ARC4 Encrypt and decrypt 16 bytes in multiple parts 2
depends_on:MBEDTLS_ARC4_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_ARC4_128:128:0:16:

ARC4 Encrypt and decrypt 16 bytes in multiple parts 3
depends_on:MBEDTLS_ARC4_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_ARC4_128:128:1:15:

ARC4 Encrypt and decrypt 16 bytes in multiple parts 4
depends_on:MBEDTLS_ARC4_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_ARC4_128:128:15:1:

ARC4 Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_ARC4_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_ARC4_128:128:15:7:

ARC4 Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_ARC4_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_ARC4_128:128:16:6:

ARC4 Encrypt and decrypt
22 bytes in multiple parts 1
depends_on:MBEDTLS_ARC4_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_ARC4_128:128:17:6:

ARC4 Encrypt and decrypt 32 bytes in multiple parts 1
depends_on:MBEDTLS_ARC4_C
enc_dec_buf_multipart:MBEDTLS_CIPHER_ARC4_128:128:16:16:
-----BEGIN CERTIFICATE-----
MIIDBjCCAe6gAwIBAgIBSDANBgkqhkiG9w0BAQowADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTQwNjA1MTU1NjUzWhcNMjQwNjAyMTU1NjUzWjA0MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxEjAQBgNVBAMTCWxvY2FsaG9zdDCBnzANBgkqhkiG9w0B
AQEFAAOBjQAwgYkCgYEA3RGKn5m6sGjKKuo7am1Zl+1OyVTkDe7OoH2gHqroDsK7
E0DbihKOiRMkpcX1+tj1kNfIysvF/pMdr9oSI3NSeUYauqBXK3YWMbOor+c4mwiL
Y5k6CiXuRdIYWLq5kxrt1FiaYxs3/PcUCJ+FZUnzWTJt0eDobd5S7Wa0qQvaQJUC
AwEAAaOBnzCBnDAJBgNVHRMEAjAAMB0GA1UdDgQWBBTu88f1HxWlTUeJwdMiY7Lf
p869UTBjBgNVHSMEXDBagBS0WuSls97SUva51aaVD+s+vMf9/6E/pD0wOzELMAkG
A1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NMMRkwFwYDVQQDExBQb2xhclNTTCBU
ZXN0IENBggEAMAsGA1UdDwQEAwIFoDANBgkqhkiG9w0BAQowAAOCAQEAGUdim4uy
/rBDFMF8qhjH1qsv0o8ON4HgP3YXbdKdIMfd+p5KtoqHQnrkixWxaIvfORnR4mGm
f8H5BimwIkNLxy7zS88TVDOYel8g7B2yl0nq4biki83NStNBYZJjxKT0ud5O5mGd
jHdy9vTEc7h8q+SHzRdgpNFXyKY5OQYng1LHco8h1UR8/nmPMuDtocHMnmMXu68a
69+TtZxx90/V4gJZOoL1iCi8HEsKoJzm/L8ji54OYt7FxgFfE3VmLsXeMaWYO8GS
BUxh5kqZ25O8hQXK5ywfuVK83Do/SsoClbgx9mboybseGVFIJaxs9e66GFDMoI3B
09JqWv4DoLNnwg==
-----END
CERTIFICATE-----
CTR_DRBG NIST Validation (AES-256 use df,True,256,128,0,0) #0
ctr_drbg_validate_pr:"d254fcff021e69d229c9cfad85fa486c":"c18081a65d44021619b3f180b1c920026a546f0c7081
498b6ea662526d51b1cb583bfad5375ffbc9ff46d219c7223e95459d82e1e7229f633169d26b57474fa337c9981c0bfb9

1314d55b9e91c5a5ee49392cfc52312d5562c4a6effdc10d068":"":"":"34011656b429008f3563ecb5f2590723"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,0,0) #1
ctr_drbg_validate_pr:"7be87545266dadd1d73546c0927afc8d":"a7f38c750bd6ff41c4e79f5b7dd3024d58ca3f1f4c09
6486c4a73c4f74a2410c4c9c5143eb8c09df842ba4427f385bbf65c350b0bf2c87242c7a23c8c2e0e419e44e500c250f6
bc0dc25ec0ce929c4ad5ffb7a87950c618f8cee1af4831b4b8e":"":"":"d5b1da77f36ce58510b75dfde71dbd5d"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,0,0) #2
ctr_drbg_validate_pr:"3771416b162f4d9c5f48a05b7aa73938":"d20a0e5cdb714f01b48e00bae51909f345af05de1321
7e5d55fc6c2d705aea550420d9a458594d825b71e16b36130020cf5948fe813462061c1a222d1ff0e1e4b3d21ae8eee31
d3260330d668d24ef3c8941b8720e8591b7deec4bd35a3a1f1a":"":"":"3cbd7d53ac1772c959311419adad836e"

CTR_DRBG
NIST Validation (AES-256 use df,True,256,128,0,0) #3
ctr_drbg_validate_pr:"f2bad8f7dab3f5886faa1cf6e1f52c87":"4df54a483b4510ed76049faae14b962fbb16459d1f6b4f
4dbeca85deded6018361223c893f9442719c51eb5695e1304a1c2be8c05d0846b6510a9525a28831a8efcbd82aa50540
d7e7864e2b8a42d44380cdc6e02eebb48d0b5a840b7cdd6e04":"":"":"0062d822bc549bea292c37846340789b"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,0,0) #4
ctr_drbg_validate_pr:"1c5760aa0fd4ce308735b28682b67246":"89defd4445061c080e4762afac194b9f79c4bb1ed88c
961af41d9d37bd388a1d45c82ca46f404348a2ae5e22ce00aa35ebc7c5051d8800890d44d25284489efcbd1f5e2b16e40
3f6921f71bbdfcf7b9aeddef65bc92fbd1cb9e4ea389aee5179":"":"":"3baf81155548afca67d57c503d00a5b4"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,0,0) #5
ctr_drbg_validate_pr:"b72b9451a5e866e226978623d36b3491":"2713d74affed98e3433559e17d240288bb1a179090
4cd7754cad97007e205a157b8ddca704a3624413f2ec8361ccd85442fb0b7cc60a247f0fd102cef44677321514ea4186d
0203ab7387925d0222800ce2078c4588bc50cdfccbc04fbecd593":"":"":"047a50890c282e26bfede4c0904f5369"

CTR_DRBG
NIST Validation (AES-256 use df,True,256,128,0,0) #6
ctr_drbg_validate_pr:"91b955a3e7eccd7f07290cba4464baff":"b160465448894c7d5ee1963bb3e1a2f3f75fcd167ffa3
32c41c4c91c1830b7c07413bd580302958aa6fa81588ad2b3173698a4afafda468acb368dbbd524207196b9a3be37ac2
1ba7a072b4c8223492ee18b48551524d5c3449c5c8d3517212e":"":"":"af2c062fedb98ee599ae1f47fc202071"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,0,0) #7
ctr_drbg_validate_pr:"d08114670c4f6016a4cf9d2da3e3a674":"38dfbfb52c185acf74de00b5a50f0cd9688286747ab3
40cfe9ad30d38b390fd2443bfd7ea93941d8262ae0f66b0eab4ff64ba59a2ff940c3c26fda103e0d798dbcaa1318e84214
3975673af8408b5af48dfbaa56ca4f9ddc87100028b4a95549":"":"":"55030fef65c679ecaffb0dc070bfd4d2"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,0,0) #8
ctr_drbg_validate_pr:"e2af9abe8770e33798a5f05b22057d24":"88fb2a8020e604ea64a620f4704078857062cc97e246
04c30de4c70cbf5e5bea0f0db79d16f4db636a2d6cd992c5890389a40cfe93967eac609e5b9f66788944285758547c713
6ef2ee3b38724ed340d61763d0d5991ece4924bb72483b96945":"":"":"a44f0cfa383916811fffb2e0cfc9bfc3"

CTR_DRBG
NIST Validation (AES-256 use df,True,256,128,0,0) #9
ctr_drbg_validate_pr:"ae30f1642753c5cb6e118d7ff5d59f1d":"340def3420b608420d81b4ea8252a3d86d3e1dd7597e
6063ed923a73a7b8e981e6079f7f0c42deb9f4ef11d2f3581abadf44b06d882afdc47896777ce8dafd85ec040f7873d0e2

5c4be709c614a28b708e547266ac8f07f5fdb450d63bc0c999":"":"":"c7e7670145573581842bd1f3e0c6e90b"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,0,0) #10
ctr_drbg_validate_pr:"711ecfe467d6f83bcc82e566729669af":"21d6c822706d1af09e4d233c0ebac7f4ec60c7be2500dd41a85a19b2dc5c7da27f8a82164bd2a644218cb5ac283c547da1064784413eed5ecf32fadd00357abaae81225ac8d0391ead533362cff56798825445d639b0b45e0312aa7047c00b4d":"":"":"d3a0d2c457f5e9d1328a9e1d22b6eaf6"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,0,0) #11
ctr_drbg_validate_pr:"f9b22152bc0eff1ebf0bfafeea40aecf":"4ee32f0aeadb3936e17f1aa3b18c10f773def5f83500c2ba96f84408a2521c1258f6be9aa5cee528746629aa2b8118ac41dd98ef1b3de31d26b8c2ad3442081203f5ef21df409df3381fbf2e064fbaec64d731dc93b3218e34bb3b03bfd88373":"":"":"86009b14c4906a409abe6ca9b0718cbe"

CTR_DRBG
NIST Validation (AES-256 use df,True,256,128,0,0) #12
ctr_drbg_validate_pr:"5174e76e904ff1471367ccace9c66ed9":"fa81535670275e8ab74121377cf88a4742dd0d7a99cf06eb9c2b4fe2b03423dbe441201144c22a9fc0ca49f5ef614987a2271cc1089d10ee01b25163c090a1f2637970e4f130920cdc3b890a078e8abbb070ded2e8fd717f4389f06ff2c10d180":"":"":"18d6fcd35457d2678175df36df5e215d"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,0,0) #13
ctr_drbg_validate_pr:"73c372f60519e8eca371eaa13fb54f88":"930c290a797b85d58b52d0d92356436977b2f636f07d5a80c987fb7eea6b750cceb9eb87860547ab4029865a6810fc5c3663c4e369f290994461d2e9c7160a8b5985853bd9088b3e969f988fe6923b3994040eeee09ad353b969d58938237cfe":"":"":"f62c7cfbe74555744790bcc7930e03c3"

CTR_DRBG NIST Validation (AES-256
use df,True,256,128,0,0) #14
ctr_drbg_validate_pr:"75ba8ddeef24f9f5b00b426a362c4f02":"7065d128ddb2fc6ea31f4110b6c0934ed112c51d74a4a0741a0843d8befac22902a01353322674c3d58935144a0f8f171a99dbeab71272ff7518c46cc7ebb573adbf95bff8ec68eeba5e8ec1221655aed8420086bda89c7de34f217dce73ccab":"":"":"700761857ea2763e8739b8f6f6481d1c"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,0,256) #0
ctr_drbg_validate_pr:"14051b57277bc3d3bbae51bdecfb9f5d":"82c80d922c47bbec0f664dd623e22a11a3b84d308351e45e30ee286e89547d22c43e17b3ca0fa08f77eef1001ba696932e9ee890e7aac4661c138e5b5ce36773d3120c35f8c94e0a78ffbf407a63ca435392e17c07461522fdc1f63f037aacff":"b70e7c1c4b8e0f1770e05b29a93f9d7a6540f23ab84136b05b161d85e5f19251":"5a737c128bd69f927f8f3ad68f93f6356d5f4ec0e36b6b50ced43dcd5c44dbc2":"a4e6c754194a09614994b36ecce33b55"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,0,256) #1
ctr_drbg_validate_pr:"4526b268128ea35f8558b4e1d08388f2":"952f3f179cbbda27ebd30f4fc31bf96baccb2adbaa9c090bc0f37044a44e85b3bc668cd3533faaf56b5da9242844d65733f7ac1f55c38b175749b88e18d19672b7bdab54e0ababdd4519fb07e0c25578f64ad40d0beb0a26275d5e2f4906aa70":"6b167c7cebea2e585ab974b60c4d305a113102ca8c3dc87651665728c4c675ad":"a038f1ca1f420eae449791f13be4901bfb91e41e052e02635b1f1817bd8969b1":"745ec376282e20fd1f9151f7040ed94a"

CTR_DRBG
NIST Validation (AES-256 use df,True,256,128,0,256) #2
ctr_drbg_validate_pr:"c1aafa90f394e0ba9a528032dc6780d3":"75fd042bfd994de2c92e5aa505945ec93bd7cf366d86a356723fca3c9479ee17fb59c6ca8ba89784d43f06cdad113e5081e02427ee0714439d88dc1a6257fc91d99c1a15e92527847ab10883cc8f471cad8cf0882f5b6d33a846a00dee154012":"c704164ce80a400cb2f54d1b2d7efa20f32b699fa881

bfc7b56cfd7c4bee1ea6":"f3baff4b6f42c8e75b70c2a72a027b14a99ae49a5a47c7af0f538843c94e1a69":"7af9113cd607cdb4c6534f401fe4e96c"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,0,256) #3
ctr_drbg_validate_pr:"e6e726b72e7b264a36ec0cd60d4578b5":"0c3c6dd706076d6484478347559b495d7ee898c39cde06027bc99f7bf69ce1140ca04602265e1308af6dd6446a1cf151749b22a99e8a05d30cc3ccd00e663bc1bc37e08ee62834fcc52a4bc8c1d6442544187484f81dc729417d5bedfcab5a54":"d84b978483c0bd8f8c231d92ea88ac21e6e667215804b15725a7ed32f7fc5dd7":"9a8971f6c559f7f197c73a94a92f957d1919ad305f4167c56fe729d50e5754a5":"e16ee5bceca30f1fbcadb5de2d7cfc42"

CTR_DRBG
NIST Validation (AES-256 use df,True,256,128,0,256) #4
ctr_drbg_validate_pr:"0272d86db283244eb7ee0ed8c8054b89":"a08ce39f2f671e1f934821a8db9070f39a734a7a20e70307fccca17db15bb4e8a421600df11d1a6e7806a14826739322c8043649ea707180f1d00dea752c2c36398030519465864c4d38163f5b0dd5be07dbc0ae29693ad4a67ca69f28414634":"aa97055cf46ba26465dfb3ef1cf93191625c352768b2d8e34459499a27502e50":"dddd0007eb29fdf942220e920ca0637db4b91cbf898efd2696576ff6bfacb9d1":"9db0057e39ca6e0f16e79b4f8a0ed5c7"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,0,256) #5
ctr_drbg_validate_pr:"4ad8f72a0d0e28a758722b20e3017d7e":"89af36a1c53f730c1b818b26aa510627b17e6f9da51c8e53930de883b7cc7a3e8c3c463c910646ac3ff08f05bca8e340daf9a322d133ae453fdf7e6860a27ff4495c89875431ba9de3e4f3247cda8c62acc86f7066448f639d8ba8b5249337f8":"9d060b7ed63bdb59263c75ebe6a54bf3a4ac9c9926ca8fb49caa905a2651eead":"016099232dc44bb7cdb492f4955ab1aabc5dc0b5731447cea2eb1d92e41482d1":"4b658e95adae4bf0c418fded4431c27f"

CTR_DRBG
NIST Validation (AES-256 use df,True,256,128,0,256) #6
ctr_drbg_validate_pr:"aa19b944c2e1b9d27933bc87322bdf14":"dc8c60dd42c85fed86cb32af035bbde5737526eb07991397c853256f2f0cb311bce70e1c5e32fc3510402d7d7e3de36fa5e584234daf391bc53cc651e001ab7fcf760679b3c82057f9d09bfdcab8e158d4daa63b20c0e1102f7a06bf5a2788dd":"6b98fec5f7de8098ff9df80f62473c73831edace832a767abf5965ea8bf789ba":"cc998bd5752f9c96ec35d9658cc8b3833dd6ab80c7accd6777c06c2cf7c01e59":"fc58833e0e27f7705e4937dd2aadb238"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,0,256) #7
ctr_drbg_validate_pr:"10c8c17a25041e2ef0d3cc80671e4cfe":"513fb96b6164ece801e52855aad28cb80131e7872d8432d27a974fb62d8d0100bb7ebcb8f5c066e230377a8847d6798c3d8090469b9719a80ac956ac33186b00eb8ca64c5530421f93932bc7c98ee92651e85dab562483bdb189676802726647":"240f36a0a598fe2116ffa682824f25acc35132f137f5221bc0ff05b501f5fd97":"22a5eb5aa00309a762ab60a8c2647eebe1083f8905104b5d375ed1661b4c8478":"145a16109ec39b0615a9916d07f0854e"

CTR_DRBG
NIST Validation (AES-256 use df,True,256,128,0,256) #8
ctr_drbg_validate_pr:"cea0c3c12be683c0f27693650a6a3d7d":"df8bc70e45fe14abb02c1b9a9754c37497fc2f67709edd854196fc4d074b12797ce7cb292f14cb1d6904abf32bf229299db5ccf5a791a3b8cd3e40a64f38f6b57df759a863e09d7676d2f3ff2762cdab221151000dba32a67f38cab93d5b7a55":"bf2ac545d94e318066ff88f39791a8385e1a8539e99ac4fa5a6b97a4caead9d4":"846efef8672d256c63aa05a61de86a1bbc6950de8bfb9808d1c1066aef7f7d70":"8d8f0389d41adcac8ca7b61fc02409c3"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,0,256) #9
ctr_drbg_validate_pr:"1b782af2545352631983dc89945ffc37":"51930fb7095edef3fc20aca2a24127f03d3c4b983329e013ad8a35016f581dd7b2d11bafbf971c1fdefd95a0024195e6e90a60ec39b1a8dbe0cb0c3aabf9cf56b662efc722b2dffa6c3be651f199cbc3da2315b4d55aeafd1492283889e1c34f":"1b6295986f6fb55dc4c4c19a3dba41066fdc0297d50fb14e9501ba4378d662ed":"6e66ff63fc457014550b85210a18f00beab765f9e12aa16818f29d1449620d28":"78dfcb662736a831efaa592153a9aff9"

CTR_DRBG
NIST Validation (AES-256 use df,True,256,128,0,256) #10
ctr_drbg_validate_pr:"6580f6df5c8de7c4a105c11ed44435c2":"d37403db6f84a7ba162e1cc351fe2e44d674ae8606280c9dac3e3975f30cbe1c9925e502a9804b91aada5cc97b259b90ccb5b8103394d9a28f0709fc9b5ffe9d73ad3672e02064ea68cebe3face5d823ee605c46c173db591135f564558dab4c":"97486a5e6ce6c6cf9d3f9a313d346cbc34b2bd54db80c5f8d74d6f6939f89519":"8377fcb52556f9974f1aa325d6e141d7b81355bd160abbc86e0007571b3c1904":"77031d3474303470dca9336b1692c504"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,0,256) #11
ctr_drbg_validate_pr:"f5303f148d6d6faca90aa88b07ab2ba9":"a0de51b8efa44b8245dba31d78f7840b2b7abced4e265b4cd9628eabc6ebbccb0f118dd8cc958b36dc959e22c4a03dafa212eeedec7d25ee6c5961187bee83b1ed3a75c7bdd9d0713b16cc67e68231f4cb274c8f3dfcc7e5d288c426a0d43b8f":"8d1fddc11dbad007e9b14679a5599e5e8a836197f14d010f3329d164c02d46d6":"9ceb6570568455d42a7397f8ca8b8af7a961a33a73770544cca563c04bc919ca":"9882f0bd1f6129a78b51d108e752b2d9"

CTR_DRBG
NIST Validation (AES-256 use df,True,256,128,0,256) #12
ctr_drbg_validate_pr:"5a799c58985aa2898cc8fe8e5bc4a9f8":"dbdbef9d217e9051025c321b628c1cc823d508ffdd13fc4edbe8677658a57ef5b64395a6b7d62c0e93dc0956ee0217ec48ae054f1d4680023cc1b2af666efa9e1458cf6b0dae72eef2392e93687bd1fb5f366bb2cdd12937ad09724e39db4189":"8c179b35739e75719e74f7c3e038bc06eb3e212d6ade85275cfebf12b2dce2a2":"af617f2e228adde3edaf52a7e5979476dbb9cd2956a1737d93a16563bbbb4888":"49a04f3b4ef052747c7f4e77c91603e8"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,0,256) #13
ctr_drbg_validate_pr:"8f5b51983a8156a529f559ac3afebbf0":"bf22b182d39622e941017285adbdfe446c3d1a72601d0e5a15674f3b1b260170b1b2ab6b588a0267d86776a5d4ce80e132d7135a581af75ea6de65153680e28ce35ce78d0917b4932000d62260149e5a3ae72bc250548390b664f53c697dac45":"4cbb5b2d6e666d5dd3dd99b951ea435cae5a75d2e1eb41a48c775829b860e98b":"a4b4171c2592516404434932ad0a8ee67bd776a03479b507c406405b3d8962bc":"cab49631733f06e3fb3e0898e5ad22e7"

CTR_DRBG
NIST Validation (AES-256 use df,True,256,128,0,256) #14
ctr_drbg_validate_pr:"9f305a77cbaec1ab408cfc0eb89c6cbb":"1e50fada1e76a0d243e6f64c36a173ddc1f47a1dab834f5cd492568792958d5be22cce3110c8e8958b47f07b5c63f86b254942361d4d553e47d36103f47cd7f0bbee27d2e238b1d85671afe8284ee1fd2a431a5f69b2df73e95341c3a2e4fe4b":"c254f3b40e773eb09053b226820f68cafa3458ad403ad36f715245a854752a93":"699e177b7be3353c45ce7b7a0d573b00087d700a9f2c1cd2e370e05d4ddadc86":"bb6b02b25a496f29245315f58a16febc"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,256,0) #0
ctr_drbg_validate_pr:"e09f65dcffc0d3a4d84bacc41617a4e46ce5184eca011049ab657566f728e4aa28315ffac166ebe50e1269b01c95b3a2":"545a783ae97d827ed0b81d9752ad0f7e965f511b1f5dae0f872e9ec37cfe63af86c1d15e153887

989b605773b16ad5505e65f617cfa8ef46547c4c3f9d0c4fd0b6e1cff5ca0f1929266fe43ba8f45ad664cfe5e90903a9cb722b42ae8989c148":"":"":"1e77d7cc18775fef9a3d3e00903da01b"

CTR_DRBG
NIST Validation (AES-256 use df,True,256,128,256,0) #1
ctr_drbg_validate_pr:"056cd44c8847d89da05fbef95e9660d589046b0c02f9b42c17fd8b069f831c73cd896005ec080113589b6f07be6e42ea":"dde6c0850fe642602eb222ca7371213c598cef8c3e71e0593ea8edb54e1bed130b9b0aebe0893093b950c52f56eb9b338aa4bd01dae030515726ece1bf751660b4a3602da6400e4b94edebba646b5c3d4e64ceea1c4f14b7a19f0142783247df":"":"":"a790ab939e63555d02ea1e9696051725"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,256,0) #2
ctr_drbg_validate_pr:"73c72c7dfe138ef4b9817d41b9722b3940762b59bda26b3f6bb8b30583e01d088a29726b71d36ffeebdb387010cb1bb6":"6fe09520e26f5abece0fceadc54913c650a9f55725af45a9a5f373d09b9970b8706b9041d0189a204f6a4eb527dfa86584a3bee3265b809c3932ae5e7228194a3cf7592fc9301c833b45a53be32b9caec9f0f91ba86519f12b0b235f68419c1e":"":"":"798d997f46ff7cc4206994085340325e"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,256,0) #3
ctr_drbg_validate_pr:"cdba7c7033c34852b7bc1a6b33edab36f41d563bd0395d1001c02ffc0c42ec8595ed2b5ddabc923372e3b6bb457833fa":"532960c23c8c8b2146576dde52fadc985134914abf42ca1c5f47206937fda41289ae5d9f935dc4ce45f77cad230a4f345599e3bae4071188324483a0b93593c96d8b6ac6c0d8b52f8795c44171f0d8cd0b1e85dc75ce8abe65d5f25460166ba0":"":"":"9d48160aca60f1a82baaa8a7d804a3d8"

CTR_DRBG
NIST Validation (AES-256 use df,True,256,128,256,0) #4
ctr_drbg_validate_pr:"02cef01aca992f60aa12db4b2c441689e4972a6f9deaf3663082afed642c1502b67b42d490af1c52c7e6eaf459882eca":"9216c9a833f81953792260a688eb7c3dfc85565ae6a6033203741a763db056247808e0ecd5ba1fc4549c3a757eba535adc786e810ddaae9a2714d31f5154f2c3ee81108669f1239f4f4efd6e18aabfa2d88f0ac25f4740108f6cfebffeb2d857":"":"":"d6378bcf43be1ad42da83780c1dab314"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,256,0) #5
ctr_drbg_validate_pr:"d7d80084e9d1fbb9315c3bce1510dbf22cf11fa54177d913a3b04b64cb30957395bd6f3d7e3d866d1be41b29db9ed81d":"80d4741e4e646748bb65e1289f1f9b3c21bffec4d0a666b301f199d76b4a83464583057079b069946b03d6ac81ebf9e6fa8d4081120f18bf58286a0c4de7576f36f3c7c353126f481a065ac28bdf28e13cd0c1e7911db6343c47d613f1750dc6":"":"":"9165a92ed92248b2d237d9f46d39bde8"

CTR_DRBG
NIST Validation (AES-256 use df,True,256,128,256,0) #6
ctr_drbg_validate_pr:"df5a68d3bede467fd69716f5f8fbac297594b8573921afb864ba76aaa6dd89e83b89e359a5a0dd1aac9b4acb9573d218":"52df6336f93781115c2a77bd8f99cb717871fe14707947a21f6093dd9205bc378acf61329f8831369b4b1af0a9edfb25d74f5863f26859ad9c920767b113c47ed2690053bf9a2f7c7a67a8d680e08865720b9e9f7b6ae697e3c93e66f24b6ddc":"":"":"c542cf248a163bbceee7b9f1453bd90b"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,256,0) #7
ctr_drbg_validate_pr:"2945527372ff71edfa5776f55f7e4a247544aa6de974e81b2eba5552843ab6dfa248695f4f3225a43d4bf3672c3a6b2e":"aa560af2132cbd0624a69c7a7e733cd59a4f2d4e61d2b830087bd88f30fa792c7e4d3168fa86a10f7619d5b9dcf4f7bb08b350ba6a6bfc0fdfb7ee7aca07260c9a11abe49963c36efaefa94d2978ed09472bf93cc873d0f24c000762bb1402cd":"":"":"33af0134eeca279dce5e69c2cda3f3f4"

CTR_DRBG NIST Validation
(AES-256 use df,True,256,128,256,0) #8
ctr_drbg_validate_pr:"b30cb767125674f6099a5cf7cb2e4f5b6c1cd1e32ffc1e393b1c5698b52b37f971f12521a7c1ffaaf3233d5391bc4c86":"2d42b00248d95d9378a2aece40d636bc1ab22edaaa64daa34335195a9efa4c1b58f13ac184ca2be52e15c3a977abde2aa505243fc106c4ea6f0671fe0f209b106ea8965645af73d8ebb8a80251db2967149c701cfe1d157cc189b03bf1bff1ac":"":"":"1e10eff9ceebc7e5f66e5213cb07fca4"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,256,0) #9
ctr_drbg_validate_pr:"c962a2da4524f08adcdd5ceddc04e669ad6154aee06164645e80c832506b98f9919451c7ec1d3a6a9704f83def8f6e2d":"a1ff68a85e437475b1b518821dbaac1730071a4ddd3255361778194fb0cfe3293e38df81527d8b8da15d03acb26467b6b53d7952441b79f95b633f4a979d998fd0417b9193023288b657d30c0cb2dada264addf9d13f1f8ed10b74e2dd2b56b3":"":"":"58990069b72b7557c234d5caf4334853"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,256,0) #10
ctr_drbg_validate_pr:"a3cc1fe561d03a055e8eedaa0e713be490c4bd4c6839a5b98c2ac0139bf215bdc46783d2a3e6b9d15d9b7a8bfe15104b":"207267911c12125cb3012230e4fafd257777ccbfb91653f77e4c1287574f9b79d81af7fb304790349dd457983cc99b48d5f4677ccd979fcc6e545cbf5b5c8b98102c9a89ae354349dbdee31a362d47c7cdae128034c0f4c3e71e298fe1af33c6":"":"":"ffd1d259acd79111a6fb508181272831"

CTR_DRBG
NIST Validation (AES-256 use df,True,256,128,256,0) #11
ctr_drbg_validate_pr:"ecf186071b81e0ed384d4ebfb5bf261b4054e2e6072b51d21dfb6817adc51ff1c8956ff3612767538cdc8d73fade78b3":"3b9aec9f8bf8495004c5e4e731e5c347988e787caf003f001e68584e3510a6abdedffa15895702c2d57c304300f4f0af80a89bcc36b3cea2f08a0740236b80cfd2ea6e5cfe4144bc4ae09270fb6bc58c313dbaaedc16d643fc0565171f963222":"":"":"a2d917f5ec39a090b55d51713006e49d"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,256,0) #12
ctr_drbg_validate_pr:"3fcedba86089709aa638d00713150df781d4a93e85f155338e90ff537bcbf017f37a2d62259f5d8cc40ddfb041592539":"6b1e9d45c2ec598de7527b6414a339f26192fc4e3f5eff4b3a3e2a80ee0f2e9743031804d1be12b3c7ff6fbc222db1d97226890addeef0e1579a860e2279292c2f769416b7068f582f6ffc192ae4c4f1eeb41d5f77f0a612b059c47aef8e3d8e":"":"":"aa414799c51957de97c0070fb00eb919"

CTR_DRBG
NIST Validation (AES-256 use df,True,256,128,256,0) #13
ctr_drbg_validate_pr:"f4c45fb8f58b7ebf73a0cd81c6a26686977558d4b8bf1cedfc6bd3754de6aaed5008fd72208437c54d8feb9a16ce3224":"6d170cf472ea07da6146a7087ed15d3f5b6ad72b8c99e46bae3b89e49a6e63467199ee16096516c2362dbd181bf5343a29fd0932d72eeb019fc3bfea3a3b01ffc2b985e341cfb6479d9dc71e2197b5cffc402587182e5fe93b5a8cf75eac2e42":"":"":"f557f627688fe63c119cf0f25274aa74"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,256,0) #14
ctr_drbg_validate_pr:"7120742a7807b66c5a9b50995d5494a5b9451bb795393c0d8a30ae665879269408f8297d49ab87410a7f16a65a54b1cb":"c08a6f9797ea668cd14ba6338cb5d23c0921e637e66a96259f78e33e45aafd035edb44394cb459453b9b48beac1e32d3b6f281473cda42fb6fd6c6b9858e7a4143d81bfc2faf4ef4b632c473be50a87b982815be589a91ca750dc875a0808b89":"":"":"521973eac38e81de4e41ccc35db6193d"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,256,256) #0
ctr_drbg_validate_pr:"add2bbbab76589c3216c55332b36ffa46ecae72072d3845a32d34b2472c4632b9d12240c23268e8316370bd1064f686d":"6168fc1af0b5956b85099b743f1378493b85ec93133ba94f96ab2ce4c88fdd6a0b23afdff162

d7d34397f87704a84220bdf60fc1172f9f54bb561786680ebaa9bf6c592a0d440fae9a5e0373d8a6e1cf25613824869e5
3e8a4df56f406079c0f":"7e084abbe3217cc923d2f8b07398ba847423ab068ae222d37bce9bd24a76b8de":"946bc99fa
b8dc5ec71881d008c8968e4c8077736176d7978c7064e99042829c3":"224ab4b8b6ee7db19ec9f9a0d9e29700"

CTR_DRBG
NIST Validation (AES-256 use df,True,256,128,256,256) #1
ctr_drbg_validate_pr:"8964ebde61f0c4e23f8e91244ae9682ed0b17e424edd4c025b461a2d209a538583f29465df3f89
cf04f703b771ff5c90":"4db8e8a27fe7a0378e37d4cc01b6a465d34be91f48c52fdc1023ef2ea1241082f522805bc8777f
da6c10e3d441b58f648edcd7d4df3df8c8a398d7b005c4fd6f41c9b033bd38fc5f577069251529b58273f6a9175feb397
8798fdeb78a043232":"5eb3fb44784f181852d80fcf7c2e3b8414ae797f7b9b013b59cf86b9d3a19006":"3eec358f7f9e
789e4ad5a78dd73987addbf3ae5b06d826cec2d54425289dc9af":"9a66c015d2550e3f78c44b901075fabb"

CTR_DRBG
NIST Validation (AES-256 use df,True,256,128,256,256) #2
ctr_drbg_validate_pr:"98784aa794df5400890e6803f06d886aeb0833b1fea28a5f7952397aa21092ceafdb9194079f36
09bc68233147c778e7":"7338521e8e127e70da259b37f5f5cdf83079bdb4024234b8ceecfba8d8c3f1c8510ff91f3bd08f
2c54f11b534048a320a15ba0fccec8da34d4ef7f49ade4847814c859831907992d0adab27046324d4d9a853eb986b8de
25b34ea74eb3d11048":"b14c5314aac11cb43f45730e474b84fbf5d1480d94d0699b80e3570f6636aa72":"d62089123
48236feee1d258092283dd9db75899769dd109cc2f0f26d88dcc6bf":"5ec75fdd1ed3a742328e11344784b681"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,256,256) #3
ctr_drbg_validate_pr:"fe9b7df306c4ccd02afd6142c6650418325617945147de436a55e78aa45866116d6678e013a0e2
c5a13e0d01fbd84039":"c4da56f4239fde0bc49b1d852cb36c80205f9e99e5995a80be04bbbba15f25b8d054c397a34cf
f1326a71f0acc4f7942795cabc3fa46339dc54b4bf7f11c095af8503004d97c485acec8815d1404674592c896ecfabefcbf
222f4fe5a3ced0af":"086d09a6ee20c69bf5c054ebc6250f06097c8da1a932fb3d4b1fb5f40af6268a":"44e64b14c49ebb
75c536329bb41ab198848849ca121c960db99f7b26330b1f6d":"7aa3a7e159d194399fc8ef9eb531a704"

CTR_DRBG
NIST Validation (AES-256 use df,True,256,128,256,256) #4
ctr_drbg_validate_pr:"c0d47ee2328185df2c299d270e11fee26df753a5b4f899fdc0dff79eb50748232f9f79cf3f5e9bd4
a26a48e743843b02":"a6b5dd5f1bad95331caae5852be50a26267af655c98feb8b66c45a8ae2ddfca270ab0d8023e43e6
e22a7b5904d63482f045e85556b9c105cde0f3eb7b1fff1026086c80b195196803b5f664362b659578894d6551fb7c45
66eec02202fdc298f":"3b575d028046e7f6005dfcdfcdcf03ff77a9cacd2516bcdff7f3601a9a951317":"f13b58daed46f5
bf3c62b518ab5c508dd2bc3e33d132939049421ff29c31c4f0":"8469dfa89453d1481abedd6cc62e4e44"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,256,256) #5
ctr_drbg_validate_pr:"a0db812a939fbf3942b00be018cff4578b9fb62629c766a50f3518fe634100b1cbc4244ae843fe3
2125c53b653705457":"7e3dca20a7a977b6616a684e309015cf6a37edd0d85819fe91d074c915b0c9540a8aa486f5868
5b064851d6164150b1c1b0e2e545c6358d28b2f5263b2fd12c503d271ab6de76d4fa4c604cae469335840328008d8ce5
545586b9ea6b21da4f9":"554b297bc32866a52884fabfc6d837690de30467b8f9158b258869e6f4ed0831":"4f688cba5
908e0699b33b508847f7dac32f233e6f02cf093efdacae74259f3b6":"9696dd6ed5875cdef4a918a6686455a8"

CTR_DRBG
NIST Validation (AES-256 use df,True,256,128,256,256) #6
ctr_drbg_validate_pr:"ff6cd20443a32c9e938f2a617bbb969ba54040b12723b0d452a669b584ba16ffaacbe38af62b5a6
2e0c67d165d022344":"efcf7536f32932526fe82b3a2333508404727878723fc09cbd902581d82463cf6acf1ddf4217ea
6404469193e8db0e7e8c864ae655b49c6a095f80f1ab16985453f0fb729c119d8a3b820034626a93b1f70eb99b6cd8c9
90dda34a1c6a4b6eea":"8d412208091b987ee0781ff679c50dbab9ef389156f570f27aaf3e699bdade48":"501381ce5e7

718c92ee73e9c247965dd5f0bbde013c4b5e625e9af8907e40566":"4f323934adb8a2096f17d5c4d7444078"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,256,256) #7
ctr_drbg_validate_pr:"bd14779153ed9696d3e5143c50b2050b6acd3ea2f8b670ef0e5f4bedf01705727bf9e64ae859214abe6ef497163f0236":"bfb0931b05a3fe232614e1b1c3060b3b07fb75d23ac10190a47a7245a6ecad5f3834e6727b75acc37e9d512d01a4a9cef6cb17eb97e4d1d7c1df572296972f0437a89c19894f721cbe085cf3b89767291a82b999bf3925357d860f181a3681ce":"0b5dc1cdfc40cfdc225798da773411dc9a8779316ceb18d1e8f13809466c6366":"843eb7297570e536b5760c3158adb27c0c426c77d798c08314f53b59aa72d08b":"1e703f3122455a40536c39f9ea3ceaa6"

CTR_DRBG
NIST Validation (AES-256 use df,True,256,128,256,256) #8
ctr_drbg_validate_pr:"64b155fd4b8634663a7e8a602e2b9fe2477be74692643ccfd0b316a025ea6f1fc0dfd0833248cb011082be36cba3c5d1":"a5b15cb1e039d7bbe2db80a32d4f402c7d3c59a45b05255401d1122770dbdb9894841964d5cadc9ae9af007d63e870d0510078885ca402bd222f16d2d27892e23292b65cf370b15d5e5a739ddd13e3e27f7c2e2b945f8e21897c3bbf05d8b043":"aea2fe995be77dfdca6ebaa1c05ba4c84d0e6b9a87905c398a3dfe08aeb26d38":"f4e9e7eb0eea4e2d419de6ad2909d36ec06c79097884bf98981e86dedae366ba":"4a28955dc97936b1c0aed0751a1afed5"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,256,256) #9
ctr_drbg_validate_pr:"e6c08e8b8d8e418477087911610096f7e0422083a376a77198e9c60fb2dc8c14aff33d7835878b65322f1561738b1ebb":"d4e0347c2158b882eb1e165f7f2aa1324d6606fe259ca730b2a3367435cb93b89108e49bd97355215063f63e78e8926b264c8a97571fd4d55882364915b7bd544254c25c2b67cdd979737c7811bcdeef5b052d8fe05a89b3291ef669d5579a61":"6607541177bc0c5f278c11cb2dcb187fc9f2c9a9e8eefa657ba92dee12d84b07":"7a439c8593b927867cfa853949e592baea0eeb394b0e2fe9ab0876243b7e11e2":"420888122f2e0334757c4af87bbc28a4"

CTR_DRBG
NIST Validation (AES-256 use df,True,256,128,256,256) #10
ctr_drbg_validate_pr:"4413ff775c9b7d9a3003e0b727e34554e0f615471d52aeb4a059777b372d60332a1a4bcaf906e598581bc5a369b2c933":"a21cf567362fed0edddfd0b1c2d85ff6d2db5484fca8bf90a82da2ab76efcac9286e417628496f37effda150ef4912125aac68aac72e6f900a70192d4ef0b4cc4e9419c93ffb245965ae30c5f8abe20f732d76080bde5a1c6b3f075eb35622d1":"b924d145fc3ecd76f000f12638ef0a49a5d4cf887aa93fc9e5c536febc454f2d":"73dbb40b257e6598744f9107c8e7ff51a080407fc9e80d39d9a4db94f167c116":"84457ea753771ad7c97ce9c03ab08f43"

CTR_DRBG
NIST Validation (AES-256 use df,True,256,128,256,256) #11
ctr_drbg_validate_pr:"5e409d56afb6940f9ffa45e0f92ef4972acedd3557b8e0f5418e302f2720ae5289294176045ad3096ea68db634cf5597":"c5a63c886af7ed7496473a6ae2f27f056c7e61c9aca8c5d095af11b2efe1a6b43344f92b37c7b6977ddbef1273e9511d9305fcbe7f32bc6a62f28d34841350362d2717dd00467224a35985b9fecc2739acd198743849dbfa97f458e2e7d6b1dc":"7fda133a23e929b17548a05013ff9c7085c5af9c979057b8f961ba7514509ff3":"bd061292b6bc3d3e71ed01af091f0169f70f23862efccd9e76345ff607dff3ec":"75b35dab3ad5e35c10ee39529a7f840f"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,256,256) #12
ctr_drbg_validate_pr:"ed2a52169791d7c7d332cf258ea4847c359335f9a6839ee767a8f76800ba28e94858cc9b7f526e62a93603fa2b1caa6b":"0a6155ff422ff6ae9814f81bf353bd3454d0c9892f9f3d730dcd8c87626f813cbe1dff1922fe73e4a319be53f4ec05e965c27f239b1e51869069a7e7cdd916fc1fd6f640bfe4b761a8040f8db37fb5ee7508e7d226c7695fb2a8bd791fe49ef2":"14073a1b4f07f3b594fa43d0c8781b8089dd2d9b8ad266e0321aaa6b71a0d058":"4247fc6886e8657b84369cf14469b42aa371d57d27093ee724f87bf20fa9e4e6":"f2aea2bc23e7c70f4ee2f7b60c59d24d"

CTR_DRBG

NIST Validation (AES-256 use df,True,256,128,256,256) #13
ctr_drbg_validate_pr:"f0d3a46501da7ab23d8688725f53f4289ce3bfa627646fe301533ec585f866caafb8131e95460566270f68cd25e1f153":"223d49f99a56cfcf2eb8cca39a8a82ee306c6272d521257f3d7d2a87699111e442fc55a399994d57373141f2207d43a8bbc1e086d67343b7dc2a891853c860fe43fb6be32cf035aca582bf5590cb5001b09b4976ea617fa7bd56da81fdef2df9":"7d12673cad5ad5003400fb94547e2b987e934acf6b930c0e7aec72634bfb8388":"e8583b9983b3ac589a6bb7a8405edfc05d7aa5874a8643f9ac30a3d8945a9f96":"ce72c0ea0e76be6bc82331c9bddd7ffb"

CTR_DRBG NIST Validation (AES-256 use df,True,256,128,256,256) #14
ctr_drbg_validate_pr:"1e4644df1d01f9a0f31d1d0c67bc9fb9a1ee2223fbfb25520d3881cde2b183b73fe1a8cc5f17796cf22aaaed57607420":"cdac62b5e4ccee8609b1f4b7a8733e69068c71219b6292ecb318b9d3479516807af280cfa20e455d5e96eb6794a3b963957f3c099fd1e1199706d36a06011836af890f3b7b15cda6346a06fdd0f194de40bfbec12b021b02eeabaa34d35b30a3":"8169251ea55cce534c6efd0e8a2956d32ed73be71d12477cea8e0f1ab8251b50":"865d14cb37dd160a3f02f56ac32738f9e350da9e789a1f280ee7b7961ec918a7":"ff11ba8349daa9b9c87cf6ab4c2adfd7"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,0) #0
ctr_drbg_validate_nopr:"1b54b8ff0642bff521f15c1c0b665f3f":"5a194d5e2b31581454def675fb7958fec7db873e5689fc9d03217c68d8033820f9e65e04d856f3a9c44a4cbdc1d00846f5983d771c1b137e4e0f9d8ef409f92e":"":"":"":"a054303d8a7ea9889d903e077c6f218f"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,0) #1
ctr_drbg_validate_nopr:"90bc3b555b9d6b6aeb1774a583f98cad":"93b7055d7888ae234bfb431e379069d00ae810fbd48f2e06c204beae3b0bfaf091d1d0e853525ead0e7f79abb0f0bf68064576339c3585cfd6d9b55d4f39278d":"":"":"":"aaf27fc2bf64b0320dd3564bb9b03377"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,0) #2
ctr_drbg_validate_nopr:"4a2a7dcbde58b8b3c3f4697beb67bba2":"58364ceefad37581c518b7d42ac4f9aae22befd84cbc986c08d1fb20d3bd2400a899bafd470278fad8f0a50f8490af29f938471b4075654fda577dad20fa01ca":"":"":"":"20c5117a8aca72ee5ab91468daf44f29"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,0) #3
ctr_drbg_validate_nopr:"911faab1347ae2b3093a607c8bc77bfe":"2f044b8651e1c9d99317084cc6c4fa1f502dd62466a57d4b88bc0d703cabc562708201ac19cdb5cf918fae29c009fb1a2cf42fd714cc9a53ca5acb715482456a":"":"":"":"aae0c0ac97f53d222b83578a2b3dd05d"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,0) #4
ctr_drbg_validate_nopr:"f959f1bc100ae30088017fae51289d8e":"77d0f0efbc7ca794a51dff96e85b8e7dfd4875fbfb6e5593ae17908bfbddc313e051cb7d659c838180d834fdd987ae3c7f605aaa1b3a936575384b002a35dd98":"":"":"":"5d80bc3fffa42b89ccb390e8447e33e5"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,0) #5
ctr_drbg_validate_nopr:"45a8bb33062783eede09b05a35bd44dd":"6bb14dc34f669759f8fa5453c4899eb5ac4e33a69e35e89b19a46dbd0888429d1367f7f3191e911b3b355b6e3b2426e242ef4140ddcc9676371101209662f253":"":"":"":"0dfa9955a13a9c57a3546a04108b8e9e"

CTR_DRBG NIST Validation

(AES-256 use df,False,256,128,0,0) #6
ctr_drbg_validate_nopr:"0ada129f9948073d628c11274cec3f69":"b3d01bcb1ec747fdb7feb5a7de92807afa4338aba1c81ce1eb50955e125af46b19aed891366ec0f70b079037a5aeb33f07f4c894fdcda3ff41e2867ace1aa05c":"":"":"":"f34710c9ebf9d5aaa5f797fd85a1c413"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,0) #7
ctr_drbg_validate_nopr:"052a5ad4cd38de90e5d3c2fc430fa51e":"98482e58e44b8e4a6b09fa02c05fcc491da03a479a7fad13a83b6080d30b3b255e01a43568a9d6dd5cecf99b0ce9fd594d69eff8fa88159b2da24c33ba81a14d":"":"":"":"3f55144eec263aed50f9c9a641538e55"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,0) #8
ctr_drbg_validate_nopr:"004cd2f28f083d1cee68975d5cbbbe4f":"6238d448015e86aa16af62cdc287f1c17b78a79809fa00b8c655e06715cd2b935bf4df966e3ec1f14b28cc1d080f882a7215e258430c91a4a0a2aa98d7cd8053":"":"":"":"b137119dbbd9d752a8dfceec05b884b6"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,0) #9
ctr_drbg_validate_nopr:"f985b3ea2d8b15db26a71895a2ff57cd":"50d3c4ecb1d6e95aebb87e9e8a5c869c11fb945dfad2e45ee90fb61931fcedd47d6005aa5df24bb9efc11bbb96bb21065d44e2532a1e17493f974a4bf8f8b580":"":"":"":"eb419628fbc441ae6a03e26aeecb34a6"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,0) #10
ctr_drbg_validate_nopr:"100f196991b6e96f8b96a3456f6e2baf":"d27cbeac39a6c899938197f0e61dc90be3a3a20fa5c5e1f7a76adde00598e59555c1e9fd102d4b52e1ae9fb004be8944bad85c58e341d1bee014057da98eb3bc":"":"":"":"e3e09d0ed827e4f24a20553fd1087c9d"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,0) #11
ctr_drbg_validate_nopr:"88f55d9ba8fef7828483298321133fec":"16f9f5354d624c5ab1f82c750e05f51f2a2eeca7e5b774fd96148ddba3b38d34ba7f1472567c52087252480d305ad1c69e4aac8472a154ae03511d0e8aac905a":"":"":"":"07cd821012ef03f16d8510c23b86baf3"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,0) #12
ctr_drbg_validate_nopr:"126479abd70b25acd891e1c4c92044f9":"70afbc83bf9ff09535d6f0ddc51278ad7909f11e6f198b59132c9e269deb41ba901c62346283e293b8714fd3241ae870f974ff33c35f9aff05144be039d24e50":"":"":"":"0f90df350741d88552a5b03b6488e9fb"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,0) #13
ctr_drbg_validate_nopr:"a45f2fca553089fe04e7832059dc7976":"5e5a9e1e3cb80738c238464ede1b6b6a321261a3b006a98a79265ad1f635573bba48dccf17b12f6868478252f556b77c3ec57a3bf6bb6599429453db2d050352":"":"":"":"6eb85ae2406c43814b687f74f4e942bc"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,0) #14
ctr_drbg_validate_nopr:"52dbb43241002415966eaec2615aba27":"31cfe60e5ed12ff37d7f2270963def598726320c02b910b5c6c795e2209b4b4a95866c64cb097af1d6404d1e6182edf9600e1855345375b201801d6f4c4e4b32":"":"":"":"2a270f5ef815665ddd07527c48719ab1"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,256) #0

ctr_drbg_validate_nopr:"176200bb44808b5400b24e1b5f56cf73":"f84d395b1734eac4600dbc36f6b1e1599bc7f2608dc8ecb3a55369d7b1b122a09f5ac9c16d9a2be37d2ff70a9bba732fc3785b23ff4ade3c8404da3f09f95a8f":"aef28c9169e9af74c73432d4aa6f5dff9ea4a53433de2ecb9bf380a8868c86e1":"0626ae19763c5313b627a8d65cf1cfba46dfd6773242738b9b81fde8d566ade1":"63c160ed6a6c1fffd0586f52fa488a9055533930b36d4fa5ea3467cda9ffe198":"e8f91633725d786081625fb99336a993"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,256) #1
ctr_drbg_validate_nopr:"19c3d16197ac93bf58c4110c9e864804":"50755cc0178c68ae70befd7744f6f1e3f6a59b3bbe484a744436079c7fae8d83c4965516fb952c63e1d0561d92cccc56037465815c9e549c9adce4a064877128":"5cb82d2c297404f3db1909480c597dd081d94ca282ba9370786a50f3cbab6a9b":"96d130faf1a971920c2bf57bcd6c02d5a4af7d3c840706081e4a50e55f38bf96":"1b0d04f179690a30d501e8f6f82201dbab6d972ece2a0edfb5ca66a8c9bcf47d":"4628b26492e5cb3b21956d4160f0b911"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,256) #2
ctr_drbg_validate_nopr:"4b1edd0f53bf4e012def80efd740140b":"e50c31ebbb735c4a53fc0535647ae1fff7a5ac4fa4068ba90f1fa03ca4ddedecd5b1898d5e38185054b0de7e348034b57067a82a478b0057e0c46de4a7280cd9":"e7154ec1f7ac369d0bd41238f603b5315314d1dc82f71191de9e74364226eb09":"9444238bd27c45128a25d55e0734d3adafecccb2c24abdaa50ac2ca479c3830b":"ab2488c8b7e819d8ce5ec1ffb77efc770453970d6b852b496426d5db05c03947":"a488a87c04eb1c7586b8141ed45e7761"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,256) #3
ctr_drbg_validate_nopr:"1f89c914649ae8a234c0e9230f3460f9":"5e029c173dc28ab19851a8db008efbcf862f4187fca84e4e6f5ba686e3005dba5b95c5a0bcf78fb35ada347af58ec0aca09ed4799cd8a734739f3c425273e441":"b51f5fd5888552af0e9b667c2750c79106ce37c00c850afbe3776746d8c3bce1":"9b132a2cbffb8407aa06954ae6ebee265f986666757b5453601207e0cbb4871b":"f1c435e2ebf083a222218ee4602263872a2d3e097b536a8cc32a5a2220b8065f":"a065cc203881254ca81bd9595515e705"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,256) #4
ctr_drbg_validate_nopr:"0ef2be2d00a16051404fc2a0faa74fdc":"b66c882ae02c5215ed3bcd9e9a40934b09bf48a15fe7558c9d9ceb0ebec63625ea18f7c3ab341d9f7edd8e1d8816edecb34dbd71ae02771327b5ebc74613dadd":"1ebe9893957a5c4a707793906d31bb201e88d88a22abd6baa6461fc61def7ffb":"f81e26744834413cb95af8d438d0050c7c968f929a33e35ee5c6715a0a520950":"687a848b2b6c715a0e613b3f3bb16cf2f056543eb9dd6b8aee8de8aa6fd8a1e6":"a6c4a7e99d08cc847ac0b8c8bcf22ec0"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,256) #5
ctr_drbg_validate_nopr:"eb2439d156c4f51fb1943c26f27de8af":"ad153fd266d9f73b21f4e5e88d3d13ba8325abdec427d5d8f671cfccdbd3510e9774d59a14d9b5472b217b7bcf355436a51965d2dff7c4ac586ab812f20d326e":"e24bd6b69a40fa0a02cefbbaa282f8f63a80e154be338d1b913418d4ff7a810d":"fd40baf11d7cdd77641a2b46916cb0c12980e02612ef59fb6fe7dabbbe7a85c0":"a40019e3b85d7d5775e793dd4c09b2bdc8253694b1dcb73e63a18b066a7f7d0c":"7cd8d2710147a0b7f053bb271edf07b5"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,256) #6
ctr_drbg_validate_nopr:"b23796d88ee5ae75ff2ba4fbbd5e2de8":"b249d2d9b269b58c5355710aaae98be12d8fb2e79046b4e6deeec28adad7e789999847e20de11f7c3277216374f117e3e006bdf99bb8631aa4c4c542cd482840":"79f0214b6b0c5ffb21b1d521498b71d22c67be4607c16300ab8dde3b52498097":"582be1e080264b3e68ec184347a5b6db1e8be

1811578206e14ad84029fe39f71":"f5e9c3356810793f461f889d8c5003b1c0b20a284cb348301ce7b2dd7a1c7dd7":"1aa8cf54994be6b329e9eb897007abf0"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,256) #7
ctr_drbg_validate_nopr:"081db0b1620a56afd87c2fd2bebb1db3":"3f1e90d88870a0bd03364036b655495e3e7d51bf67fb64ba0cbf003430af5585f5936b84ab3b8a55c02b8b6c54bea09cf2d77691858c5818991383add5f0c644":"5b98bc83ae8bed5c49cb71689dc39fee38d5d08bdfa2a01cee9d61e9f3d1e115":"aad3e58fdd98aa60fc2cae0df3fc734fff01a07f29f69c5ffeb96d299200d0d8":"bad9039ebb7c3a44061353542a2b1c1a89b3e9b493e9f59e438bfc80de3d1836":"8d01e3dc48b28f016fc34655c54be81f"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,256) #8
ctr_drbg_validate_nopr:"a8427443d9c34abcdcca061a2bbcff52":"b0e9b2192adc8912653d90a634d5d40c53ca4383290a8764bdf92667f859d833c3e72ad0ff41e07fe257b1ead11649be655c58a5df233114e7eda2558b7214d7":"c6cad9fb17ada437d195d1f8b6a7fa463e20050e94024170d2ffc34b80a50108":"be461a9c1a72ebaf28ee732219e3ca54cbee36921daaa946917a7c63279a6b0e":"b6d110d6b746d7ccf7a48a4337ba341d52508d0336d017ae20377977163c1a20":"16ccd63dbf7b24b6b427126b863f7c86"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,256) #9
ctr_drbg_validate_nopr:"86bd02976e6c50656372b8c212cf0a7a":"89900b0febf6b4e19ab8fc5babb4122a8aad86d658d0c2f98988c99fbd8530ff4ad365bd5fddaa15f96537bd72deb5384405b610e6ebae83e848307051fd6c82":"41bf3794ee54647a48a2588fdfdea686f1af6792e957d42f181f2631b207ac0c":"c4478afbea4eecb225448f069b02a74c2a222698c68e37eb144aff9e457f9610":"41a99e0d3f5b767f9bedcb2f878a5d99d42856bed29042d568b04e347624bf7f":"863337529aac9ab1e9f7f8187ea7aa7d"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,256) #10
ctr_drbg_validate_nopr:"e809ef8d4c3d82575833d51ac69481b2":"3e831b7715ce202c95ec85337e2c0061d972169955bd96fbe1f758508c0336b3226260ea5e66f943b538eb115ffe4d5e534cbe58262a610528641629bc12fc75":"4d40c6a961168445c1691fea02ebd693cb4b3f74b03d45a350c65f0aaccb118b":"b07dc50e6ca7544ed6fdebd8f00ed5fa9b1f2213b477de8568eb92dddaabfe3f":"cbac982aa9f1830d0dc7373d9907670f561642adb1888f66b4150d3487bf0b8d":"2814be767d79778ebb82a096976f30db"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,256) #11
ctr_drbg_validate_nopr:"ad71caa50420d213b25f5558e0dc1170":"6a3fd23e7dc934e6de6eb4cc846c0dc3cf35ea4be3f561c34666aed1bbd6331004afba5a5b83fff1e7b8a957fbee7cd9f8142326c796ca129ec9fbacf295b882":"3042dd041b89aaa61f185fdda706c77667515c037f2a88c6d47f23ddadc828ae":"9b1e3f72aaab66b202f17c5cc075cfba7242817b2b38c19fe8924ca325b826ea":"8660b503329aaea56acdb73ca83763299bac0f30264702cb9d52cbaf3d71d69d":"c204a3174784d82b664e9a1c0a13ffa6"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,256) #12
ctr_drbg_validate_nopr:"5fd6606b08e7e625af788814bef7f263":"baf8750e07194fc7172c736e0fdea0a632810d45602dff17ce37adf106d652f87e31b6bd24d21481c86444d8109586118672a6f93731b7438a3f0f39648b83a3":"3c37193d40e79ce8d569d8aa7ef80aabaa294f1b6d5a8341805f5ac67a6abf42":"c7033b3b68be178d120379e7366980d076c73280e629dd6e82f5af1af258931b":"452218a426a58463940785a67cb34799a1787f39d376c9e56e4a3f2215785dad":"561e16a8b297e458c4ec39ba43f0b67e"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,256) #13
ctr_drbg_validate_nopr:"08def734914ecf74b9eccb5dfaa045b8":"6697f889fcf6dae16881dc1e540e5c07f9461d409ac
ee31842b04f93c00efbba670dfbf6040c1c2e29ad89064eae283fd6d431832f356e492bc5b2049f229892":"a6ac87af21e
fd3508990aac51d36243d46237b3755a0e68680adb59e19e8ae23":"0052152872b21615775431eb51889a264fed6ca4
4fa0436b72a419b91f92604c":"ebadf71565d9a8cc2621403c36e6411e7bed67193a843b90ccf2f7aa9f229ca2":"c83fa
5df210b63f4bf4a0aca63650aab"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,256) #14
ctr_drbg_validate_nopr:"6437862e93060def199029ff2182f1e5":"719d1afcb6dc8ca26cba6a7c10f59cf82345b2a0c63
1a7879812d6f2d2663b49f9e92daecb81ff7c0790205d66694526477d6de54a269f542cb5e77fe4bc8db3":"5c961db0ac
2ea8caf62c9acc44465dcfb4d721fcb2cd3e1c76cdcb61bfaa7e75":"24eabd392d37493e306705d0b287be11a4d72dd4b
9577ac4098ef0dae69b0000":"9e4f05c1b85613e97958bc3863e521331b2bd78fdf2585f84607bf2238e82415":"21aaa
e76dc97c9bf7cf858054839653e"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,0) #0
ctr_drbg_validate_nopr:"cd7a1981c1b7079c1c38f5aeee86db22207cb9faed8c576b1724ca7817aa6abfb26c42a019eb
4c2f4064f0587ea2b952":"7f88c3805ae0857c5cbb085a5d6259d26fb3a88dfe7084172ec959066f26296a800953ce19a
24785b6acef451c4ce4c2dfb565cbe057f21b054a28633afbdd97":"":"":"":"76c1cdb0b95af271b52ac3b0c9289146"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,0) #1
ctr_drbg_validate_nopr:"0ccdac2fd65a86bf8f8e9ddcabffb9d29a935139f627c165a815b23137eeee94cbb21be86ac51
17379177d37728db6fd":"6f61703f92d3192cd982b2e52a8683e0d62918d51b12e084deae06c4a8e08ecfb3d2d30a980
a70b083710bc45d9d407966b52829cf3813cc970b859aa4c871fe":"":"":"":"e6c73e159d73c2ba8950cd77acb39c10"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,0) #2
ctr_drbg_validate_nopr:"fbbcc4abfd671296de3e0dcf409a139e35deae126c1941bf1afcc8d3da3a2d65f54a6d317bb6d
683a3a77f6266b007ff":"c662ed723e7041877542fdcf629533d4a74393eb4dae4f3ec06d2d1c0d37ed7f519609a8485c
b8deb578ae4cbb45c98ef7f2f2e677363e89fb3744286db6bfc1":"":"":"":"9d934d34417c6d0858f4a3faacbe759e"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,0) #3
ctr_drbg_validate_nopr:"1b824790b6b22b246bcc1bcfbbb61a76045476672f917b72e79cca358e650eb29ed49fb0a57
39e097f5f5336d46fc619":"c57a5686486ebacc2422236b19110c754795a869a8157901cf71303de1adc6af16a952190a
395d6c20e155e690f41922f6f721dc8e93da81afb844f68714cba7":"":"":"":"13e7bf23d88f3bb5a5106a8227c8c456"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,0) #4
ctr_drbg_validate_nopr:"2ea7861e374232cb8ceecbbd9a18fc1f63c31f833fe394f1e19c8ef61092a56f28342fa5b591f7
b951583d50c12ef081":"6a0873634094be7028b885c345cd5016295eec5e524f069de6510ae8ac843dba2cc05c10baa8
aad75eac8e8d1a8570f4d2a3cf718914a199deb3edf8c993a822":"":"":"":"c008f46a242ae0babad17268c9e0839a"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,0) #5
ctr_drbg_validate_nopr:"39caa986b82b5303d98e07b211ddc5ce89a67506095cad1aeed63b8bfe0d9c3d3c906f0c05cf
b6b26bab4af7d03c9e1a":"f2059f7fb797e8e22de14dac783c56942a33d092c1ab68a762528ae8d74b7ad0690694ede4
62edbd6527550677b6d080d80cdabe51c963d5d6830a4ae04c993f":"":"":"":"202d3b2870be8f29b518f2e3e52f1564"

CTR_DRBG

NIST Validation (AES-256 use df,False,256,128,256,0) #6
ctr_drbg_validate_nopr:"a4e25102c1b04bafd66bfe1ce4a4b340797f776f54a2b3afe351eede44e75c28e3525155f837e7974269d398048c83c3":"0a03b7d026fab3773e9724dacb436197954b770eca3060535f2f8152aa136942915304dede1de0f5e89bd91d8e92531b5e39373013628fea4ee7622b9255d179":"":"":"":"be21cab637218ddffa3510c86271db7f"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,0) #7
ctr_drbg_validate_nopr:"6de33a116425ebfe01f0a0124ad3fad382ca28473f5fc53885639788f9b1a470ab523b649bad87e76dee768f6abacb55":"d88312da6acbe792d087012c0bf3c83f363fa6b7a9dd45c3501009fb47b4cfcfeb7b31386155fe3b967f46e2898a00ecf51ec38b6e420852bef0a16081d778cc":"":"":"":"2c285bfd758f0156e782bb4467f6832c"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,0) #8
ctr_drbg_validate_nopr:"b8ab42fd3f6306426602cae0c48eb02ffa7053940389900c17846e1d9726251762095383f2ec3406b3381d94a6d53dd8":"6a7873ccb7afb140e923acbec8256fa78232f40c0c8ba3dcbcf7074d26d6d18a7e78fffda328f097706b6d358048ee6a4728c92a6f62b3f2730a753b7bf5ec1f":"":"":"":"13504a2b09474f90d2e9ef40d1f2d0d5"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,0) #9
ctr_drbg_validate_nopr:"042b524444b9903c1ecb80af21eef0e884115561a15a1ab2f9f3a322edcbf14174f54d315196a632940c2c6f56612c09":"31ba5f801aeaac790f2480fbd2373a76ba1685ebebc5ae7cd4844733ec3cfb112634b3899104dcc16050e1206f8b3fb787d43d54de2c804fd3d8eb98e512bb00":"":"":"":"0a0484c14e7868178e68d6d5c5f57c5c"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,0) #10
ctr_drbg_validate_nopr:"632758f92efaca39615862177c267906ab0424230d481ee0a5aa1a5f66697d3918d4aab3f310b72a7f2d71c0a96b9247":"46dc837620872a5ffa642399213b4eebfb28ca069c5eaaf2a636f5bd647de365c11402b10ecd7780c56d464f56b653e17af8550b90a54adb38173a0b2f9e2ea7":"":"":"":"90432ce3f7b580961abecde259aa5af6"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,0) #11
ctr_drbg_validate_nopr:"7b389118af3d0f8336b41cf58c2d810f0e5f9940703fd56a46c10a315fb09aafd7670c9e96ffa61e0cb750cb2aa6a7fe":"76e92e9f00fc7d0c525c48739a8b3601c51f8f5996117a7e07497afee36829636e714dbcb84c8f8d57e0850a361a5bdfc21084a1c30fb7797ce6280e057309b7":"":"":"":"7243964051082c0617e200fcbbe7ff45"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,0) #12
ctr_drbg_validate_nopr:"e50d38434e9dfe3601e7ea1765d9fe777d467d9918974b5599ec19f42d7054b70ff6db63a3403d2fd09333eda17a5e76":"c9aa4739011c60f8e99db0580b3cad4269874d1dda1c81ffa872f01669e8f75215aaad1ccc301c12f90cd240bf99ad42bb06965afb0aa2bd3fcb681c710aa375":"":"":"":"28499495c94c6ceec1bd494e364ad97c"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,0) #13
ctr_drbg_validate_nopr:"3253cb074d610db602b0a0d2836df1f20c3ee162d80b90b31660bb86ef3f0789fa857af4f45a5897bdd73c2295f879b6":"b06960a92d32a9e9658d9800de87a3800f3595e173fdc46bef22966264953672e2d7c638cc7b1cada747026726baf6cea4c64ba956be8bb1d1801158bee5e5d4":"":"":"":"b6608d6e5fcb4591a718f9149b79f8f1"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,0) #14
ctr_drbg_validate_nopr:"83e4733566f90c8d69e6bcbe9fb52521ff3e26f806d9b7b86e9344cca0305dbf106de855240f1d35492cc6d651b8b6ae":"0e0105b12af35ac87cb23cf9ca8fb6a44307c3dcdc5bc890eb5253f4034c1533392a1760c98ba30d7751af93dd865d4bd66fbbeb215d7ff239b700527247775d":"":"":"":"68d64d1522c09a859b9b85b528d0d912"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,256) #0
ctr_drbg_validate_nopr:"a94da55afdc50ce51c9a3b8a4c4484408b52a24a93c34ea71e1ca705eb829ba65de4d4e07fa3d86b37845ff1c7d5f6d2":"a53e371017439193591e475087aaddd5c1c386cdca0ddb68e002d80fdc401a47dd40e5987b2716731568d276bf0c6715757903d3dede914642ddd467c879c81e":"20f422edf85ca16a01cfbe5f8d6c947fae12a857db2aa9bfc7b36581808d0d46":"7fd81fbd2ab51c115d834e99f65ca54020ed388ed59ee07593fe125e5d73fb75":"cd2cff14693e4c9efdfe260de986004930bab1c65057772a62392c3b74ebc90d":"4f78beb94d978ce9d097feadfafd355e"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,256) #1
ctr_drbg_validate_nopr:"e8649d4f86b3de85fe39ff04d7afe6e4dd00770931330b27e975a7b1e7b5206ee2f247d50401a372c3a27197fec5da46":"78d7d65c457218a63e2eb1eba287f121c5466728ac4f963aeaabf593b9d72b6376daea6436e55415ad097dee10c40a1ff61fca1c30b8ab51ed11ff090d19ef9a":"cc57adc98b2540664403ad6fd50c9042f0bf0e0b54ed33584ee189e072d0fb8f":"ab2f99e2d983aa8dd05336a090584f4f84d485a4763e00ced42ddda72483cd84":"0ecd7680e2e9f0250a43e28f2f8936d7ef16f45d79c0fa3f69e4fafce4aeb362":"08e38625611bb0fb844f43439550bd7a"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,256) #2
ctr_drbg_validate_nopr:"6c79e1556889b3c074fc083a120d73784b888c5acb877899f17ce52e424b84178d144441aa9f328c730a951b02b048df":"c78ff6b9fc91cbce246c9fcc2366d5f7dd6d99fb1325d8997f36819232d5fcd12ccafdcbefd01409d90acd0e0ffb7427c820b2d729fe7e845e6a6168fc1af0b5":"60cba10826de22c5e85d06357de63d6b2ff0719694dafca6ab33283f3a4aacdd":"8943c22fb68b30811790a99b9cbb056e1a2c329185a199c76ba5aeceb2fcd769":"70671a50e8387bf232989d904c19215c7535ad2d0c5dec30a744c8d2706be6ec":"f6b94b671cae8dfa8387719bfd75ee84"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,256) #3
ctr_drbg_validate_nopr:"f5ab77b2a8e370548b88febfd79772144cd5fc8d78062582addd4ff1e5c10094b390e66b3c4efb087510de1b9d25703f":"21a21c9314b37d4ade4a50a5d85995e0be07e358ed9bca19daa867a8d47847105dca7a424f32f715adb8fea5d3a41cfe388872a42ab18aa5cbcd7bde4adc3f8b":"023d582569a7ff1405e44cf09ceebb9d3254eef72286e4b87e6577a8ab091a06":"39597519872d49fbd186704241ba1dc10b1f84f9296fb61d597dbd655a18f997":"3091c9fe96109b41da63aa5fa00d716b5fa20e96d4f3e0f9c97666a706fa56f1":"1fb57058b3ba8751df5a99f018798983"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,256) #4
ctr_drbg_validate_nopr:"f0b79e292d0e393e78b6d6117e06d2e725823fe35bde1146502967a78d99d6bca564f0e2f324272f968be5baab4aeb29":"192054dddac02157a35eb7f75ae8ebdb43d6b969e33942fb16ff06cd6d8a602506c41e4e743b8230e8239b71b31b2d5e3614e3a65d79e91d5b9fc9d2a66f8553":"b12241e90d80f129004287c5b9911a70f7159794e6f9c1023b3b68da9237e8b7":"59e9c3c0f90e91f22c35a3be0c65f16157c569c7e3c78a545d9840f648c60069":"089a59af69f47ddb4191bd27720bb4c29216f738c48c0e14d2b8afd68de63c17":"15287156e544617529e7eede4aa9c70e"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,256) #5
ctr_drbg_validate_nopr:"e3f33843aecb35d01001ff92ab9a0f1a5431ba9de3e4f3247cda8c62acc86f7066448f639d8ba8b5249337f8c353bbbd":"ef081af1f62400a3d193969d689a40234998afb646d99a7c4b9cbbf47e650cda93a90e754a16fffa25fc2a2edab09720b4520c47309ec4f6d9f76f0162af6cae":"e7cc55b72862544a8661b5034e15587b1e5a45eb5dc744f5fa1db9b267f1c3ff":"882d30c888eb8e344b1d17057074606fe232ceb42eb71055264ede7bb638f2a2":"9ce65e95c1e735fe950e52c324e7551403d0ef70ad865bd31fef1e22b129fdd6":"205e3a53367c4a5183be74bb875fa717"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,256) #6
ctr_drbg_validate_nopr:"f30a18d597d8591a22dee908de95c5af74884b025f39b4f6707d28447d9d0a3114a57bc2d9eed8e621ec75e8ce389a16":"fae3d554d12a14e29de1b622922f27559559ca1518c9f800375a37a212e8b9a653cc370022

3e9404d5bf781d15fccf638050a1394592caba001cfc65d61ef90b":"54240edd89016ed27e3bb3977a206836f5ef1fba0f000af95337d79caca9cf71":"250611e51852d933ff1a177b509c05e3228cb9f46dfb7b26848a68aad2ce4779":"f8b602d89fa1a0bfb31d0bd49246b458200a1adb28b64a68f7c197f335d69706":"7b63bfb325bafe7d9ef342cd14ea40a4"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,256) #7
ctr_drbg_validate_nopr:"c8dbc3d39beb612811c52e2b46ef76d2b7bd5d3a90ceddf9fb864fe6f44e36687d88158d61014e192f9a3cd474338e13":"8e60115b4af9c8e5606223792539e9ba87e9ef46cd16fcc09046db1ef8d3c036241cae5d61141711818e9e861dbd833632069ebf5af1bd6d4e513f059ab1efd3":"9b56eba0838457f736fc5efa2cfbe698908340f07d4680e279d21dd530fdc8c8":"62c47ece469a7a409e4b2b76d1c793aaf11654e177cc8bf63faff3e6c5a5395c":"4251597013d0c949c53bbd945477b78aa91baa95f1ff757c3a039ccc4e1f4789":"af2f37160940f0cc27d144a043ddf79b"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,256) #8
ctr_drbg_validate_nopr:"a37f9ed6c4e8f74ff16046b0678ef7bd24fcdca247b771ea1ce1fd48e3f5d2067e38aaf64ec59f1f49d96fa85e60ef03":"95da91f4185b254322ef0fc852473a9b9e4c274b242ded8a4eae6f1e2badde0664cf57f2128aa3dc83e436f7e80928a01d93bf25011eedf0190d0bf3619cd555":"b4a22f5598f79d34f0b9600763c081b0200ba489da7028ad0283828545c6d594":"fa3edc0962b20a9d9e1d0afcad907c8097c21d7a65c0e47c63d65cea94bf43bd":"49ba791a227e9e391e04225ad67f43f64754daac0b0bb4c6db77320943231ec3":"32f313ded225289793c14a71d1d32c9f"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,256) #9
ctr_drbg_validate_nopr:"87f85b9c19eba1d953b6613cf555c21bc74428d9a8fee15e6cd717e240506f3e80860423973a66c61820d4ce1c6bb77d":"f22dd3517350176e35e1b7ecc8c00bea4747f0ac17bda1b1ddf8cdf7be53ff8c326268366e89cf3b023a9646177a0dcca902f0c98bf3840c9cbdf5c0494bee3c":"611caa00f93d4456fd2abb90de4dbcd934afbf1a56c2c4633b704c998f649960":"cba68367dc2fc92250e23e2b1a547fb3231b2beaab5e5a2ee39c5c74c9bab5f5":"f4895c9653b44a96152b893b7c94db80057fb67824d61c5c4186b9d8f16d3d98":"a05de6531a1aa1b2ba3faea8ad6ac209"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,256) #10
ctr_drbg_validate_nopr:"9670deb707caabc888a3b0df7270942934732e02be728a4bedb5fc9ca4d675b2f3b47c7132c364ce6292cef7c19b60c7":"bba34e6f4ee27e5d4e885e59f8bbb0dc7353a8912e66637d7515a66e5398d9a8cbd328fed32f71bdd34c73cdf97e0d211be6dabfb0144e1011fd136cf01ea4e4":"9f55da36babd6ea42082f5f5d4330f023440bb864f8ad5498a29cf89757eaeab":"8013a309058c91c80f4d966f98bce1d4291003ad547e915777a3fce8ae2eaf77":"c83106272d44e832e94c7096c9c11f6342e12ec06d5db336424af73d12451406":"bc8d4d00609662c1163dca930901821d"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,256) #11
ctr_drbg_validate_nopr:"6d984c8ab923a7e118447fd53ad287b8f01d1e6112cff12bfb338ecd3ed16bafdd634677c600bdd68f852a946f45c3d9":"ed0e524ed2990ef348dbb15b3f964b12ad3109978d6952ae193b21e94510a47406926620798e71a0ffcbdd2e54ec45509d784a8bfc9d59cb733f9f11fc474b5e":"0a3a32260d04dd7a82fb0873ecae7db5e5a4b6a51b09f4bf8a989e1afacbda3b":"3cbcabb83aab5a3e54836bbf12d3a7862a18e2dffeeb8bdd5770936d61fd839a":"f63b30a3efc0273eba03bf3cf90b1e4ac20b00e53a317dbf77b0fe70960e7c60":"ab9af144e8fad6a978a636ad84e0469e"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,256) #12
ctr_drbg_validate_nopr:"2c59520d6f8ce946dcc5222f4fc80ba83f38df9dce2861412eebb1614245331626e7fb93eedbad33a12e94c276deff0a":"2882d4a30b22659b87ad2d71db1d7cf093ffca80079a4ef21660de9223940969afec70b0384a54b1de9bcca6b43fb182e58d8dfcad82b0df99a8929201476ae9":"d3c17a2d9c5da051b2d1825120814eaee07dfca65ab4df01195c8b1fcea0ed41":"dcc39555b87f31973ae085f83eaf497441d22ab6d87b69e47296b0ab51733687":"9a8a1b4

ccf8230e3d3a1be79e60ae06c393fe6b1ca245281825317468ca114c7":"fba523a09c587ecad4e7e7fd81e5ca39"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,256) #13
ctr_drbg_validate_nopr:"1c1207f50b645aaed5c16fe36f6aae83af4924e6b98a7e2a2533a584c1bac123f8b6f0e05109e0132950ae97b389001a":"8ae9a5903da32a38b7c6fed92dd0c6a035ca5104a3528d71a3eacc2f1681379724991a0053e8dac65e35f3deee0435e99f86364577c8ebdba321872973dc9790":"568bfee681d7f9be23a175a3cbf441b513829a9cbdf0706c145fdcd7803ce099":"e32cb5fec72c068894aaeabfc1b8d5e0de0b5acdf287a82e130a46e846770dc2":"d4418c333687a1c15cac7d4021f7d8823a114bb98f92c8a6dccc59ff8ad51c1f":"194e3018377cef71610794006b95def5"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,256) #14
ctr_drbg_validate_nopr:"28254014c5d6ebf9bd9e5f3946fc98e55fe351deee8fc70333e4f20f1f7719a522b3ea9a4424afe68208d1cc6c128c47":"98a0db985544c33990aee0f69655dba7198e6720ce56ff9d4662e26f0c6b4ee7ab599932c05295f6c5a4011085c5b2c861a5a8ae4f572ce614ff2dafc0fddb34":"64215cbe384f1f4cf548078ffd51f91eee9a8bae5aacdd19ca16bcaaf354f8ad":"2e21df638dabe24aebf62d97e25f701f781d12d0064f2f5a4a44d320c90b7260":"7f936274f74a466cbf69dbfe46db79f3c349377df683cb461f2da3b842ad438e":"25c469cc8407b82f42e34f11db3d8462"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,0) #0
ctr_drbg_validate_nopr:"e26c8a13dae5c2da81023f27ab10b878":"fea104f90c5881df7ad1c863307bad22c98770ecd0d717513a2807682582e3e18e81d7935c8a7bacddd5176e7ca4911b9f8f5b1d9c349152fa215393eb006384":"":"":"":"fd87337c305a0a8ef8eef797601732c2"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,0) #1
ctr_drbg_validate_nopr:"8d7dda20a9807804bfc37bd7472d3b0c":"1d723cbc2ff2c115160e7240340adbf31c717696d0fdfecf3ec21150fca00cde477d37e2abbe32f399a505b74d82e502fbff94cecac87e87127d1397d3d76532":"":"":"":"7221761b913b1f50125abca6c3b2f229"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,0) #2
ctr_drbg_validate_nopr:"c02e3b6fd4fea7ec517a232f48aaa8cb":"0820fc21cecba6b2fe053a269a34e6a7637dedaf55ef46d266f672ca7cfd9cc21cd807e2b7f6a1c640b4f059952ae6da7282c5c32959fed39f734a5e88a408d2":"":"":"":"667d4dbefe938d6a662440a17965a334"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,0) #3
ctr_drbg_validate_nopr:"9aee0326f9b16f88a4114e8d49b8e282":"ef0aae3f9c425253205215e5bf0ad70f141ad8cc72a332247cfe989601ca4fc52ba48b82db4d00fe1f279979b5aed1ae2ec2b02d2c921ee2d9cb89e3a900b97d":"":"":"":"651ad783fe3def80a8456552e405b98d"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,0) #4
ctr_drbg_validate_nopr:"1e7a4961d1cd2fd30f571b92a763c2c5":"a9262ed5b54880cc8ecd4119cce9afe3de8875d403f7ca6b8ed8c88559470b29e644fddd83e127c5f938bc8a425db169c33c5c2d0b0c5133c8f87bbc0b0a7d79":"":"":"":"1124c509ca52693977cf461b0f0a0da9"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,0) #5
ctr_drbg_validate_nopr:"ae0b0d2e84f48c632f031356cdea60ac":"554cf6fad1c376ad6148cd40b53105c16e2f5dd5fa564865b26faa8c318150bfb2294e711735df5eb86ff4b4e778531793bad42403d93a80d05c5421229a53da":"":"":"":"1212e5d3070b1cdf52c0217866481c58"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,0) #6
ctr_drbg_validate_nopr:"16b8c7495d43cd2ff5f65ad2ab48ecef":"7cffe2bef0d42374f7263a386b67fba991e59cefd73590cbcde3a4dc635a5a328f1a8e5edd3ada75854f251ee9f2de6cd247f64c6ca4f6c983805aa0fe9d3106":"":"":"":"d3869a9c5004b8a6ae8d8f0f461b602b"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,0) #7
ctr_drbg_validate_nopr:"a2d5eff6f73f98e5b04c01967dffa69b":"59759bb91b3c4feb18c0f086269ec52e097b67698f4dfe91ebe8bef851caa35cadb3fd22d1309f13510e1252856c71394a8e210fdbf3c7aae7998865f98e8744":"":"":"":"a1f99bd9522342e963af2ec8eed25c08"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,0) #8
ctr_drbg_validate_nopr:"ea1f47fe5e281136706419ea9b652967":"0ec7c617f85bec74044111020c977be32ab8050b326ebc03715bbbffa5a34622f2264d4b5141b7883281c21ea91981155a64fb7b902e674e9a41a8a86c32052b":"":"":"":"daf75b8288fc66802b23af5fd04a9434"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,0) #9
ctr_drbg_validate_nopr:"6f072c681a82c00dcd0d9dd5b7ffa2af":"cd7ce90f0141e80f6bd6ff3d981d8a0a877d0ddae7c98f9091763b5946fc38b64c1ef698485007d53251ad278daf5d4ae94a725d617fc9a45a919a9e785a9849":"":"":"":"39c0144f28c5a490eff6221b62384602"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,0) #10
ctr_drbg_validate_nopr:"9d730655366e2aa89ee09332bd0a5053":"854766e842eb165a31551f96008354bca1628a9520d29c3cc4f6a41068bf76d8054b75b7d69f5865266c310b5e9f0290af37c5d94535cb5dc9c854ea1cb36eb7":"":"":"":"baa2a3ed6fdc049d0f158693db8c70ef"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,0) #11
ctr_drbg_validate_nopr:"3363881611bfd5d16814360e83d8544f":"6abfab14cbf222d553d0e930a38941f6f271b48943ea6f69e796e30135bc9eb30204b77ab416ac066da0a649c8558e5a0eac62f54f2f6e66c207cab461c71510":"":"":"":"5be410ce54288e881acd3e566964df78"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,0) #12
ctr_drbg_validate_nopr:"14e589065423528ff84a1f89507ab519":"0d2e446cad387a962ff2217c7cf4826dcabb997ab7f74f64aa18fbcb69151993f263925ae71f9dfdff122bb61802480f2803930efce01a3f37c97101893c140f":"":"":"":"fc2d3df6c9aae68fb01d8382fcd82104"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,0) #13
ctr_drbg_validate_nopr:"974c5ae90347d839475f0f994f2bf01d":"aa04d9fc56349fdd31d868e9efc2938f9104c0291e55ac0aa0c24ec4609731b8e0ac04b42180bde1af6ad1b26faff8a6de60a8a4a828cd6f8758c54b6037a0ee":"":"":"":"3caec482015003643d5a319a2af48fb4"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,0) #14
ctr_drbg_validate_nopr:"b3a110587a16c1eafe51128a66816ecf":"203bba645fb5ccee3383cf402e04c713b7a6b6cca8b154e827520daac4ea3a0247bbdc3b2cd853e170587d22c70fb96c320ea71cb80c04826316c7317c797b8a":"":"":"":"9af4f67a30a4346e0cfcf51c45fd2589"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,256) #0
ctr_drbg_validate_nopr:"55546068cd524c51496c5fc9622b64c6":"951e712d057028158831ca8c74d4ae303c6e4641c344a1c80292260bdd9d8e2f5b97606370e95903e3124659de3e3f6e021cd9ccc86aa4a619c0e94b2a9aa3cc":"2d6de8661c7a30a0ca6a20c13c4c04421ba200fbef4f6eb499c17aee1561faf1":"41797b2eeaccb8a002538d3480cb0b76060ee5ba9d7e4a2bb2b201154f61c975":"b744980bb0377e176b07f48e7994fffd7b0d8a539e1f02a5535d2f4051f054f3":"65b9f7382ed578af03efa2008dbdd56f"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,256) #1
ctr_drbg_validate_nopr:"a0c92565640a3315cac8da6d0458fb07":"6e9b31755c1f45df7d685f86044ab3bc25433a3ff08ab5de7154e06b0867f4e3531ed2e2a15ab63c611fc2894240fdac1d3292d1b36da87caa2080d1c41bcf24":"c6c74690bdee26288d2f87a06435d664431206b23b24f426e847fb892d40d5d5":"4e7dc1adbc8bc16ba7b584c18a0d7e4383c470bff2f320af54ad5ade5f43265b":"c6fb8ee194a339726f5051b91925c6a214079a661ec78358e98fc4f41e8c4724":"c3f849ee7d87291301e11b467fa2162f"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,256) #2
ctr_drbg_validate_nopr:"63e143bd6a87065a00eea930593f9b29":"62c2c790cb56518ed2d8d65952bbd4ab85a56463495c940b94f403a93338bdc96129feea9335b1a3e0ada7cf4c207f4732013bc6a52db41407bf5d6fe9183b3c":"7b4e9ff0c8f8c90f8b324c7189226d3adccd79df2d0c22b52fb31dbb5dfefba6":"49e1aecf2b96a366325dc1892c016a5535dd2480360a382e9cc78bf75b2bba37":"f4ce1d27e759f3ba4a56aaab713642b4c56810c9995fbfc04ce285429f95a8f4":"513111abaae3069e599b56f7e5fb91d1"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,256) #3
ctr_drbg_validate_nopr:"98dc16e95f97b5b9d8287875774d9d19":"2fab4a629e4b21f27488a0c9ed36fc8e75bee0c386346c6ec59a6f045975e29818440a6638eb3b9e952e19df82d6dc7b8b9c18530aef763d0709b3b55433ddc6":"2e9d2f52a55df05fb8b9549947f8690c9ce410268d1d3aa7d69e63cbb28e4eb8":"57ecdad71d709dcdb1eba6cf36e0ecf04aaccd7527ca44c6f96768968027274f":"7b2da3d1ae252a71bccbb318e0eec95493a236f0dec97f2600de9f0743030529":"841882e4d9346bea32b1216eebc06aac"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,256) #4
ctr_drbg_validate_nopr:"5dbac5c313527d4d0e5ca9b6f5596ed7":"c00b28c78da4f9ce159741437fe7f90e4e23ecd01cd292f197202decbbc823d9ce46b8191c11e8f8d007d38e2ecd93b8bd9bbad5812aaf547ddf4c7a6738b777":"460c54f4c3fe49d9b25b069ff6664517ed3b234890175a59cde5c3bc230c0a9e":"bf5187f1f55ae6711c2bc1884324490bf2d29d29e95cad7a1c295045eed5a310":"28fd8277dcb807741d4d5cb255a8d9a32ef56a880ccf2b3dcca54645bd6f1013":"b488f5c13bb017b0d9de2092d577c76e"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,256) #5
ctr_drbg_validate_nopr:"254d5f5044415c694a89249b0b6e1a2c":"4c1cc9ebe7a03cde31860637d8222faeefa9cbf789fab62e99a98d83084fef29eafcf7177d62d55435a1acb77e7a61ad86c47d1950b8683e167fe3ece3f8c9e8":"71af584657160f0f0b81740ef93017a37c174bee5a02c8967f087fdbfd33bfde":"96e8522f6ed8e8a9772ffb19e9416a1c6293ad6d1ecd317972e2f6258d7d68dd":"3aaa5e4d6af79055742150e630c5e3a46288e216d6607793c021d6705349f96a":"66629af4a0e90550b9bd3811243d6b86"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,256) #6
ctr_drbg_validate_nopr:"b46fceed0fcc29665815cc9459971913":"ff62d52aed55d8e966044f7f7c5013b4915197c736

68e01b4487c3243bbf5f9248a4fdd6ef0f63b87fc8d1c5d514ff243319b2fbdfa474d5f83b935399655e15":"994d6b539
3fbf0351f0bcfb48e1e763b377b732c73bf8e28dec720a2cadcb8a5":"118bb8c7a43b9c30afaf9ce4db3e6a60a3f9d01c3
0b9ab3572662955808b41e4":"bb47e443090afc32ee34873bd106bf867650adf5b5d90a2e7d0e58ed0ae83e8a":"1865f
ee6024db510690725f16b938487"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,256) #7
ctr_drbg_validate_nopr:"e1a5dd32fc7cefb281d5d6ce3200f4ca":"bf1ba4166007b53fcaee41f9c54771c8a0b309a52ea
7894a005783c1e3e43e2eb9871d7909a1c3567953aabdf75e38c8f5578c51a692d883755102a0c82c7c12":"32e9922bd
780303828091a140274d04f879cd821f352bd18bcaa49ffef840010":"01830ddd2f0e323c90830beddedf1480e6c23b0d
99c2201871f18cc308ab3139":"f36d792dbde7609b8bf4724d7d71362840b309c5f2961e2537c8b5979a569ae8":"708
0e8379a43c2e28e07d0c7ed9705a8"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,256) #8
ctr_drbg_validate_nopr:"d1b7be857a422b425ae62c61e90a192a":"6ac34c4ce22b644632283ab13e294df2093e939d3
2411340b046c26fcc449d0fd6d14132c7205df303dbb663190e6e86ad12e14e145b6603308241f38d94eb5d":"aacfe85
53d5ffef6abc3fd8f94d796cae2079ff04f7ab1b41982003f02427c7a":"01d2d1bc29d6a6b52bb29bd6652be772096ca2
3c838c40730d5b4a4f8f735daa":"27af728ee07d3f5902f4e56453b6a9feb308ef14795eb5630b2651debdd36d5b":"b03
fbcd03fa1cc69db0a4e3492a52bad"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,256) #9
ctr_drbg_validate_nopr:"a2c49aa6f3f92e36266bf267af5877ed":"5684c3eb9931412707848495931 4d52b3bc50cb36
15c0eef6b48850d98aee04c528b0693be13ed1bb4040e8e96cb13c316143f0815cd68d1bb7931a3d9b88a3d":"566522
085426b76bdef152adefd73ef0f76eee4614bc5a4391629ec49e0acffb":"30ef9585148dd2270c41540a4235328de8952f
28cf5472df463e88e837419e99":"adc46e0afcf69302f62c84c5c4bfcbb7132f8db118d1a84dc2b910753fe86a2d":"4edc
4383977ee91aaa2f5b9ac4257570"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,256) #10
ctr_drbg_validate_nopr:"43852c53041a3a4f710435dbd3e4382b":"ab7bca5595084bccdba80ade7ac3df2a0ce198fa49
d29414c0249ec3d1c50d271ca74ba5c3521576a89a1964e6deded2d5ba7ff28a364a8f9235981bec1bedfa":"c5612a954
0b64fc134074cb36f4c9ea62fff993938709b5d354a917e5265adee":"eee2258aba665aa6d3f5b8c2207f135276f597adb
2a0fbfb16a20460e8cc3c68":"a6d6d126bed13dbcf2b327aa884b7260a9c388cb03751dbe9feb28a3fe351d62":"e04c3d
e51a1ffe8cda89e881c396584b"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,256) #11
ctr_drbg_validate_nopr:"52628551ce90c338ed94b655d4f05811":"b3a4a3c4d3d53ffa41b85ce3b8f292b1cc8e5af748
8286d4c581005f8c02c5545c09bb08d8470b8cffdf62731b1d4b75c036af7dc4f2f1fc7e9a496f3d235f2d":"f5f9d5b510
75b12aa300afdc7b8ea3944fc8cf4d1e95625cc4e42fdfdcbeb169":"60bccbc7345f23733fe8f8eb9760975057238705d9
cee33b3269f9bfedd72202":"c0fa3afd6e9decfbffa7ea6678d2481c5f55ec0a35172ff93214b997400e97c3":"5a113906
e1ef76b7b75fefbf20d78ef8"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,256) #12
ctr_drbg_validate_nopr:"0e4873c4cbcde280abc6711a66dbb81a":"1ab7c7d8fe8f505e1dd7ddb8e7cda962572f7004b2
a14c7a7c5bcf24bd16616e2c42c50ae5db9981ccd7d0c79062ac572d3893486bd0ae1f99cbc1d28a9e4c1e":"e4b89e28
663e853f8b380c8a4491b54121fe6927340a74342362c37d8d615b66":"619775878879eff9ee2189790ff6f187baed4ed
1b156029b80e7a070a1072a09":"ba3d673e5e41bd1abbc7191cc4b9a945201b8fef0016e4774047ee2abf499e74":"475

8fd021c34a5cf6bea760ad09438a0"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,256) #13
ctr_drbg_validate_nopr:"0684e8ef93c3363ba535c4e573af1c24":"748a5f5fde271c563a8f8d15520d6818f7ed0efb9b434adf2ff9471b391dd225b37868179ffa9a6e58df3b1b765b8945685a2f966d29648dd86a42078339650b":"e90c82153d2280f1ddb55bd65e7752bf6717fbe08c49414f6c129bf608578db7":"c17e97c93cfabe0b925ca5d22615a06430a201b7595ad0d9967cc89a4777947d":"3d554c430c8928dcdb1f6d5e5a4306b309856a9b78c5f431c55d7ebd519443bb":"d3da71af70e196483c951d95eb3f0135"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,256) #14
ctr_drbg_validate_nopr:"89b885ddb12abc4f7422334f27c00439":"e2366eec626bfd9cb932bcaa0569de6a7a37cf1dfde1f25d00d1a0c89fe25fea592cbd2af7c8202521fa48e15f7cc7e97e431b222b516a3ad2bb7b55b7fcf7f4":"c77ee92bd17939efe9bee48af66589aee1d9fe4cd6c8ae26b74b3799e35342a6":"23e80d36ca72ecc38551e7e0a4f9502bed0e160f382d802f48fb2714ec6e3315":"6b83f7458dc813ce0b963b231c424e8bced599d002c0ef91a9c20dcc3f172ea5":"81d13a6b79f05137e233e3c3a1091360"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,0) #0
ctr_drbg_validate_nopr:"ff568be02a46343113f06949a16cc7d9da315aef82f5681f0459650e5e180e65d1d77b00e5ce3e3f9eb6c18efff4db36":"77de4e5db3b308c38c814228583dfd1eb415771f4ae30f9cc2d35b48075286a4e8c2c6f441d1aac496d0d4be395d078519e31cb77d06d6f7fd4c033bc40fd659":"":"":"":"448ac707ba934c909335425de62944d6"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,0) #1
ctr_drbg_validate_nopr:"6f092b85eb9f96427642f69467911172cba6df86e0db08d04e824cde6fb91d9b9af2cea53f42d53c45ee3e69a2327172":"667d3ed9f41a154ea33b55182b8bee4d7d46eff8e890c7036cf7c2665d44c28f9e3a8cff166dabfaf262933d337e729e0b6a60a51d00ba18f877bdc9d0cc659e":"":"":"":"16a200f683ab862947e061cddaac5597"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,0) #2
ctr_drbg_validate_nopr:"26e635a6a2b6402b968c1eea13c6a980a0ee9b8497abc14fccdc5bf8439008861f74de2c200505185bf5907d3adc9de2":"80e56f9893beb9f22b2b03caa8f1861d5b31b37f636f2ccbc7e4040ad3073aa20f2f3c6bfefc041df8e57e7100794c42732b6d4b63d8bb51329ca99671d53c7c":"":"":"":"807586c977febcf2ad28fcd45e1a1deb"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,0) #3
ctr_drbg_validate_nopr:"b239c485d319ce964d69bd3dbc5b7ab9cc72ac9134a25e641bcd3c8b6f89e7e08ef2d0a45cf67667a4e2e634b32d73ff":"c963e17ef46b7b2c68756019704ec7435ec093c423600b3f2f99dd8989f8539a11b1b0598e93e84d50b65e816e794421ab546b202e4b224a8494538dda85da82":"":"":"":"2a3218b4d59f99bd3825631a6eefb09c"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,0) #4
ctr_drbg_validate_nopr:"0239545a23735b803ae7cb7766194917d6cce164f7ec4f65c6ccd5ec1db5297722d4b7466589da4d39f4585856bc1d7e":"71a440b70a2b5ce41b85de27d987fa2a0628d7990dd7cd1460fddc5410ce6e9bb0ae4f90231f45bc71188fd94e4170389a8bbe4a7e781c95c9a97ad78ba7d07b":"":"":"":"9dafaa8b727c4829dda10a831e67419d"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,0) #5
ctr_drbg_validate_nopr:"237e8916eadd65e3422fe59ab257b7e6957fe24f760b499fbd052241879e8294b01d2169ec2b98f52660d9f5170dee22":"d8908cfc1ea8518c1442e46731f30fdad85399894db262b8f4fdc0dbcbf11b60b60b25d3108f4b169fcbef621a14c635525fa3af8ccef6b91f808479509967f4":"":"":"":"593c39c56bb9e476550299ee8d85d2fc"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,0) #6
ctr_drbg_validate_nopr:"28b6639b415c79012c749dc2a0d18433ec36eda55815f0841241453fa11b9d572b7c29208e0
1dbb0be91e1075f305d7f":"6767c3eb6ba1b19412c32bfe44e4d0317beba10f3abea328cda7b7c14109b72046c8691c1
c7b28487037d381f77a3bbc8464a51b87de68bdc50ec9c658f915ab":"":"":"":"e390806219fa727e74a90011b4835ed6
"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,0) #7
ctr_drbg_validate_nopr:"ce735a8549fc3f9dfc7b96bf0d48936a711439ac7271d715a278718aca9e2fe3c801030bc74b
048ac1e40852345e87cc":"510b0dc06e84ceb901c7195c2f00ad7a04bdd75e0ab52b3d2cd47ddfcd89248dd58e3f1aa8
c1ffe306f493905f65369eaed2a5b337dff8ac81c4c1e8903a6ad5":"":"":"":"ba871ba5843083b553a57cf8defa39d7"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,0) #8
ctr_drbg_validate_nopr:"841ea92fa42c06769c5c52fe152d07837b8ff0048392caa5dd045054353d363b25439eb5885e
96771dded4005f2baf42":"97511ae52590a0b64b75c37e10b89671880d2d6e8f90780ac27263dbc0e32d0824be5e80a8
8cf8fc3d4c607eb873c0322d09b9ca3498c4015c53ca6fee890093":"":"":"":"a8fb31362bd997adf4d9116e23dbaf10"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,0) #9
ctr_drbg_validate_nopr:"55cd76fa5f004b97bb8e14170f79f52715d18c60f142b06d16e8e06c274798190a79c8b32516
3989d86323c03dbe0d68":"bafc0ba64669c9a36514bde6169034101f29e2a0a4b9a55c0aae7dff0c5aca2371b523e26dc
44bf75493bdaa023d1555294178288b70f1ae72150d9f7265b4e6":"":"":"":"fa16dbdaf01b3c202426adabf61fa64a"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,0) #10
ctr_drbg_validate_nopr:"ff3f3098fa3d2b23b38ed982e7afb61d46b4848c878b9280f8e5ed6bd81176e76f0a2a85071a4
11829cf84421c22f23e":"92194e2c700fa724489683d0b6ddcf72c89b9c3f3ff584e802ae426be4908b1ade093bcf9baf7
738b988dc0fde1739498a97c9610da853a7c83981c6a7b68096":"":"":"":"f85490426dc243ba09f9719bff73545a"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,0) #11
ctr_drbg_validate_nopr:"7242c1020a63770cccf6f8100970990232a9d11d61c9b0d38fe5e7a568a86252a66481212e5
d53c868561298dd5bdeec":"7c3806a32ccf3252ac27a92a07209cd7000b160faa70b9024420b903587d1d77f002d3abe
28b563d32ccc502b88f83bc5996f3dbbf0f57835839eadd94563b9d":"":"":"":"2232181f08c1569efaad1a82bcb5f3ba"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,0) #12
ctr_drbg_validate_nopr:"a2e445290fed8187df6d2a57e68385bb62d700cb8f140410766b53e69e6a0f2939bbfa7ce091
525c9051f064e383a2e1":"fdae5f1ea253108fcb255d215a3ce1dc1d101acf89de4423b75a74619e95f3feaa35b5e0bec4
30b0ad9567df818989c36c77742129af335c90ceb6dd79c7d2c4":"":"":"":"3841e2d795b17cb9a2081d6016a1a71d"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,0) #13
ctr_drbg_validate_nopr:"bc885454e385d911336dda9b7a609a6a7079a4a5a860fcd704161c34658bd98685bb03418b7
f24f2ed9475eb8ceb232e":"77bef884a91126564b3214029ac6842d86e4c1fa283e33d6828d428377416f66947e39a4a
6708e10bfdae8337a6f302420a6649fc109d0f094c18c1e9361375a":"":"":"":"ea20780ed280d8109f811a6a398c3e76"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,0) #14
ctr_drbg_validate_nopr:"c1825cf00cdc2da93adb3e7a33c1f3a76c49166887883744ea2683ddca23f31900f25c434364
c992a6d913f753a9c42a":"56940a6fc4823c9e42e8ffed63fc3cf46d0a2b305c236a511b0b5ec7005ecd8989bf2006ebe5

2ed55845f7cc25d3d0086cece95f0bff6fa7e17ddf474704abfe":"":"":"":"b037c7f0f85f4d7eaeeb17f4c8643a74"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,256) #0
ctr_drbg_validate_nopr:"19b83c0deea6463a3912d21ffc8d8041a5b30640352abc9652770cfca99dc53c9c09942ddd67b91f4da50a8615462ce4":"5d85c56d0d20ee39958a90f301d2f8bb136fa34d09b41a0c9375114a0df9c1dcdb2a62c4be398d9eaf2440949b806f0e5a977da608eeb652a41711d1e9b72655":"9c1db928b95c84cb674060a6d2f6b7a6a5d43e9ee967e9f821bf309ca5f8821f":"a3111cb57365c617df0b0bb3a1aada49ca789bc75903eeb21e42a7d3d0dd0825":"ce7f557c70676987d13aca60bc4585147efeed97be139871a1b29caa1e180af9":"4a49430277d64446e2fa75763eb79ec6"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,256) #1
ctr_drbg_validate_nopr:"239f21be6cda23e8660c8a5e04c79f6dad6f363ac6dcffd9228699ae43fbce5ac3c51645500cb3eae68f0b604dc4472c":"2975a099f7e6530e5576534c25171f39131d6bffb99259f7f2bbf7d77de9fb1e829052b54a9631a733113021692eba1097438347c6de82307a0c2bb308edf065":"d451a54584e6d1d634217379e7e60e67303e19dd4ba63b097899c7349a5a7433":"a33dc24c6a656eb26275415581d568b7c2424a9c5fb9e2944ca35ecbf641f713":"8dfccc62379af46844df136122b72a878d9d61b40ccaa029b09e6b9f0b4d0192":"005e91760d89ecb64b5fc3b0e222fca3"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,256) #2
ctr_drbg_validate_nopr:"e326abbe1db3ead3738d2ca4d9f1d62080cd23ff3396f43a0af992bed2420cec6661dfaac83c3c4d83347ac840f7dc14":"37c94d11ed0e93b8199d43d6eb242165dddd12fe39c0bea4cdef6bcfeb5d17bb866f080a9daef128f685fb3bc59c945927fb0aa3e17068515c3c92fbdf04a228":"1ff41405dbb3b12b8ddc973069edc2d2801af0e0dc9bde2cdd35c5b2d4091509":"138b6d2eabef4b32174afb0156ad1df570cf6e5f6ebde5d19cc30daffd9ca4f2":"f27cf7422808c54c58fcdde1cece92f5342c7a10ac43ab3b2e53362b2272e3ad":"506d6fae6fff9f222e65ac86df61a832"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,256) #3
ctr_drbg_validate_nopr:"cb0229d2bb72d910b0169e8f93318905aef8dd93ed91a2f8388545db32db3f2489e7988b50de64c49a9f7feb5abe8630":"514ec8c02439290853434e75e3d0bd159eacd5ac13b8f202cfd5c36cdc0fe99b53a1b7a1619e94eb661ac825a48ea5ef8bb9120dd6efc351e39eb7cc5223f637":"a6ed69c9216c551793107f1bdaa04944f6d76fe4474f64bb08b0ebc10a18f337":"e0bc1cc56fdfeef686e0c7ec359e2e8bd48d76c8643c40d12325328170bbf702":"87c5b23aa3c100ff9e368fc47534ff8fa2f9e2bfd3599519ee6f60164485cf6d":"bd419968f636e374268ccdd62403f79c"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,256) #4
ctr_drbg_validate_nopr:"bdd156ef3c4e09b77fe8781c446eac55b562e4ee1b7d15515a966882d4c7fadb0fc7b37554ba03908838db40499ded5b":"9facd9f4587819acb358e4936d9f44b67ddf82616e79a44ffd6a2510f652f6b9cebc1424b5c642362b19f63c615f49686df66a8f80ddffb56ce0c0d8540150fb":"35ea316fe302786f626e3831530622b62eb33a3608d4af3384ecfcbd198f3f05":"8d4fae22290b6ef8618ded1c3412e85fab7b8d17fb9cbd09dbc87f97279cc72d":"2f54928372e4ce447201427a3ae05769ae1c54b2e83bdc86d380a90b07f2890c":"8045e8da88b1bc126785c8a771db5354"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,256) #5
ctr_drbg_validate_nopr:"154876298a1b63334624b367da984eb31d7260abe79ced41de35ba68a716233a5df0937b90f89dde7fd55a9693c9031f":"36895f574e9e9d08e6c885d305eb4764c1e5689d1f99c2462b3ebdf659e8ce43818dfc886ec797843bfee361b554cd5f969b0c7b0381b53f4afc1bcadbf7eb1c":"c3a46105c50a167a5b0391053f3814a06c90cea2c1fa9329d97fdbc62887ff6d":"54c7d66c65dbddb4665981bff0f503de37d724362aeb67abce6a870fd6a7398a":"58204ca953cbd46dd6c8870b358cba77c436870db49bcd3e2f92697bb580b460":"cd903c0f11ea701214f91715cfec11a3"

CTR_DRBG

NIST Validation (AES-256 use df,False,256,128,256,256) #6
ctr_drbg_validate_nopr:"94e273fde1e699f84aeef343eb0277c50d169bb5496575301021a2be50df6a555d1422ea88e0e4d905158e93fd8d0089":"1cd97b6e6e7f19401e409aea7b3ec33a8faefd71402b8f34a73c1cb1af215e0e87debe68bce590d41c1f90c6ad9db3d30b3901862e076d765ffdf58776e5fb7e":"6ee75e9f9aee6ac93e20f742f20427e5eb9b4ad2ed06fbba8c7b7870a96941ac":"0ba60399893ede284372bc4e0a37702a23b16aa8e5fe70ea95429af87ff291aa":"94bd2b51c32d29cd14e2123221e45ec0cf1f38766fb6bb0716856d0138f6fa39":"831793686abd406f7b385cd59e497b18"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,256) #7
ctr_drbg_validate_nopr:"5a699113ebf98bff9cb780ce29747a61ba2d7581a5716065d018c89348d7c2ed3f5bba32442cd192c1e37b77b98f5791":"de6d2a3b6ad9af07058d3b1d1976cf61d49566b965eb4e9b74a4cad8e286e7a40b254b860e2e209a8cb4cff3a8e615b84f5ae7505957a758e266a4c3e915d251":"ed18c16a61ba5ecc0755f94c286390a6d46e6e26439dadd36c83ebdee42b4b4c":"7c4550d058b85580be2053fd9d933c87041c5c3f62a5b6b303259dafc90d9041":"ebebfcb9b4b3595e516939ca0688422bbdfc4b9f67b0d6619757cb315b7d7908":"1a5a496aa2268483444b3740c9cc4104"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,256) #8
ctr_drbg_validate_nopr:"42450f2689b87a3dd940f3b9e3b32d4654c725a24ddd2c22f006694321dacf1980b50f7ac0401626453ec836039bfdc9":"4765399ccbbf3d33433bb992ee29e4381f28d800b05431f1c5b3e949c5db72c582bfe8ba08db1575b866816cabbe5e1d31d8a870ceed49fb75676c97020d1f22":"6ee5a7613c25ecec263a2fd2288948b2df9a05d50040c4031b0653878fdb067f":"68a1038481be7412d6a7c8474d4b2a2535c9b55ea301ee800d5a846127d345cb":"7a1915cf78e6da2dc7840cba40390d668d07571608b77857d2224c4531c17bb8":"80a6c622e64495f9a391f5a8a9c76818"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,256) #9
ctr_drbg_validate_nopr:"873869e194201b822b140bdd7797dd1ed408f2190b759c068b7019e6707f60751e101d3465c4ec57dbf9d1ea7597fa44":"d2f92706ca3fb9ced8183c74704440d7eedee1542c2e812f65afc83f4b62dadf1c51fa68f8d5f457a893211c8afc82c93e6a1e15822eff0d4ada6efd25d271a0":"8d0393d2a1ae8930ea88773adfa47b49060f0bf2d3def2acc57786bfbd1e2d6f":"5bcf5ff4fbd9eaabf8bf82ec7c59b043fd64b0025ad1ab2b384e399b9e13147a":"6e2d05e286c90502a3abf2ee72ab7ffb520ce5facfb27e095787a09a412abec3":"e1ceda71b8feb4b0d14d35bbb57a79a2"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,256) #10
ctr_drbg_validate_nopr:"1fecb5fe87c2a208b4f193e9c3ff810954c554150d544baea1685fb4774320315d5cb651be493ef120ef6966e3e7518c":"34bc292809674352ffb60786dca59ec799188aa401b366a48cdeddf37c12ee4c666f8fb3a0d53df4cd7191166d50ff01d992f94cd92da7a385ffe5795b197ced":"38249fed34a907768eac49267c2c613a65154eec5b73b541d7d7b314b5080061":"115be9cb914b50480fffe078d8170870b56129a0a74271dee063f8b2049e1be3":"69fa6faf7223f5bb1b55f35a544f78181579b1745990053357916fe507e51db6":"60cc92d3ba3ff0715f5627182334ed1b"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,256) #11
ctr_drbg_validate_nopr:"4d283eb5ecd85a1613c975e24832770643613c9a5aee0d8649bc0d68c89cf1ea6ec3a1a22eefd9e212d602c338d64c6e":"4aa6917a5c9f370590d70536fdd89c916fec5e5bcbade8c6a6cfcf5b232c98a6b3e6b79a2dfb0778fbc3f1da7b06044d7b0fa2c04ffc3b71324aca1ee19f936b":"05a7092a684ba7a7fbd33533f9be58a4140a3855d4c5f44a31d665a0720c1739":"557ef1bedc890d1543de6cfeb25642782683d77a46bc8aa0836b07157599c7c3":"e87e45073ff8e36c38b128cd2275a160e431787b5e81f6c2fd7a37909eb72ea5":"31ecfb1bcf3253ba5f71b185a66c7cff"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,256) #12
ctr_drbg_validate_nopr:"a6f488104a6c03e354d5d1805c62dcd3016322d218747fa83f9199e20f6ab1cfbc2b889536bda1187f59b7294d557ff2":"22f8ad57a2dfa8010e2865ad6263823652917b84dfea61f639efdb0fdbb35c6341ca7721095

d69686212dffe78410c0d0db94f04756d52e7d76165d5a1d516d9":"fb9951d563f7aa88db545874b1a3049c5f79774d4
86e7a28aed1ed75f59224a5":"b1ea7c6b53e79e4e947e63086dee32dcc17bc4f27fba6142f8215ec081cdd5c9":"0d12cc
0a39bfbf87194e4070f6b54caaabbe48fa192b96cfed2a794d95fa299d":"62a1c5678e6e8fc738d375e2ca48751f"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,256) #13
ctr_drbg_validate_nopr:"9d67e017e0abdd7c079bc0354f33dab696ad64146802f06d6cefd9cdefbf55b197f5899e5efaa
269cc0432c87648ce18":"d8be0ec1119ff959c32c9cf29914e3f7bf2b01bdbf806c2d9ba119ae2a2cfb565871762b02ee
7bf68f1d280532fd7ae7368517f6f751739b228d23df2f207f35":"74a5e24477e8759bedfbaa196f398777108392efb8c6
4c65c0c9ecd6cd3b5f04":"70cbc6cfe1d6ab4bc30d66fa162d5d4b3029e4b1b9d759f3eae17fb508e91a46":"d3c538e04
2f0eb796b4af9b4e65cd850425c72e2c896fcea741c17172faf27d9":"559a5e04b75cec250aac2433176a725e"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,256) #14
ctr_drbg_validate_nopr:"10914608a6d373a26c53ab83014283b678d73dfea65b4a3540af17f2fafa3b3cf698925b423e
db9f946b906f43110795":"9ded87d289412dfda8935e5b08ec66b68abd1bae1fc5363e4341f58db954f1f9bc4b681c0d9
30ba080f85f8fd04c173cb2b77723ce67692efa7ade48b82b6926":"225159b4c679094f277516b2335b1e8b7d0a7ea33
fd56822906d481fe412586d":"4967cd401cd466aba0be5f55615ca0d9fb8adbde5cb4e6ae3a0159fcd6c36bf0":"fec14f3
25b8b458ddf3e7f2e10938f4c2d04c8d9885bb5b9277bdc229c70b354":"1cd5c0bdeb87c79235bead416c565d32"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,0) #0
ctr_drbg_validate_nopr:"b023f6a6f73d4749b36eb54867994432":"2462ad760ddbca4e013688bf61381f190c7b2de57
cbeeec81d6ab7b6f067b75adc3545887f8d2aa5d9b9dfcbfa425d610faa9c247eb5d71145f302918e908ae5":"":"":"":"c0
620c68515a4618e572db6e4c14473d"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,0) #1
ctr_drbg_validate_nopr:"7e0fcd953c1c8bb8d03d7a0e918fb59d":"56b2e11d5c2d87d2c9c90c285e0041beb4594a6ef
dd577580095612e50cf47c0b76208337e1e18453082d725629667d86226ab22944bbfb40c38b7986e489adb":"":"":"":
"7194eee0d333fa5282dc44db964ecf5b"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,0) #2
ctr_drbg_validate_nopr:"0130217d4a3945402ed99d7b8504fe4b":"28e592fd9db72b40ae4888078aedde260f6de4f04
72a7601258e694d7bb6af6810ff4eabdffb332932765fa1d66650fb78cc2be484c0ba803eb9a2502020e865":"":"":"":"4
652f0545385fdbe02d05aec21668608"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,0) #3
ctr_drbg_validate_nopr:"07854447e33521d2d997d90c0887f42d":"c561ab6acfbfb98879982ac7add92b80471e0154b
77ccc9fd98e7c2013c411e8075948e97ab4db7505797a99d456e54e6585042efeff7e3970e399ea0d27537c":"":"":"":"1
a14a810c11b4f0af23c6467c47bbde0"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,0) #4
ctr_drbg_validate_nopr:"68a8ec01581d6066391f3e5977465026":"747c7e9aace6d4f840c7b5261e0af796c51647742
1d52850a7072a0ab2c768fcc80c9ba8d18b228e77a7f6131c788a76515fe31aef4ed67376568231a4700fac":"":"":"":"a
5723c43743442fae3637bb553891aeb"

CTR_DRBG NIST Validation (AES-256 use

df,False,256,128,0,0) #5
ctr_drbg_validate_nopr:"1459038c60b70bae7af0da6cfab707a2":"9f7d839310846bd452827a185539c0eb0f106acc7bc4de80d3521a970b23483d57826b1484d329a2d1c2ecfeaf8eeffbaa6e1a305e3f1e47b96ad48a711ad1aa":"":"":"":"5fcd6bf108fe68b85f61f85c0556f5c0"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,0) #6
ctr_drbg_validate_nopr:"a3357db173df98da4dd02ee24ce5c303":"f1ce08587ac0338b4d0b8e075b42b6501e77758b30087de028a8622fb7abd7f65e3b4f802d1a472dedb9c1a6dc9263c65918d8b7fafd0ae7e9c39e2e8684af3f":"":"":"":"8a5fa11d8e78fbf1ca4e4ca3e1ae82b8"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,0) #7
ctr_drbg_validate_nopr:"212f4c80c7e9287c8d25e3b965f91a3c":"bf1d715b3f56c433827c9cb429bee5ca61c80a8d9b2fd4498e1c86ce703637f8f7f34056ab0039e0baa63320df0ec61de60354f2ece06356d9be3c6d1cdcc4cf":"":"":"":"04ac2f969e828f375b03ee16317e8572"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,0) #8
ctr_drbg_validate_nopr:"46e85752e0af82fc63932950120e4b5d":"ae4316424fa765179404188eb8839ce84ad8db92cb12f39089a93a2dbdc371e2fdbef1ad080eb354eecdda3a10ea66ef647aa095afa1786c01bd1c9f70d8da4f":"":"":"":"de576284d8ad36b31bd4f8f3da633e36"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,0) #9
ctr_drbg_validate_nopr:"ec2459b1dd7f50df63e14e40aa4a4e66":"b964a24bf98264327c0b9e2e1c99ed1b35f534be801c996f318bc2074ed2500ba8488c4feb442b507c3220523c0041c9543133379365e65e092850a5e3f96cc9":"":"":"":"4d466e2f388aae40d1b31ce1f8ddc5e8"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,0) #10
ctr_drbg_validate_nopr:"acf480d54f4c66d611519b72f2c0dca6":"d5b3277cf8badf6be86af27dd36f23ffc580847c5fcb56c4d8a42339336f185c38ffb86f4d8aa7646c1aaed6c2b0c7ae7e4d435f481d62bb01e632f6bbb2abf9":"":"":"":"746aaa5423ef77ea6b1eda47410262dd"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,0) #11
ctr_drbg_validate_nopr:"edb80fddc595b234e3c5c03b2be3d721":"94aad8c772201435543efd9013c9f5f022038db6864e9ed4141ea75beb236844da6e6a17109262bc80f528427b37d9da6df03c7dd25be233774384a7f53197ea":"":"":"":"511927f10f800445b705ea3cfe6ec823"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,0) #12
ctr_drbg_validate_nopr:"c7790c9888b0e731ca6ccd60c32bb98a":"967050c11050a6d99a5da428d1f0fc8068b29ba4c66965addbfd31b745cb07d2439d268ab32a5fa2b1934bf277ff586506a941768468905ed980537d8baa1d07":"":"":"":"978493f0cece6f94d21863a519e06dbe"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,0) #13
ctr_drbg_validate_nopr:"58c75625771df61c48a82590eeed3378":"be3120e8515a98701b4b2fb0667de2bad3f32bcbf10fb9b820956f9aa7ffa1bbbafb70002a9c7fdd1cf7e76a735261798dc60a1163919d58e39ef0c38b54b27b":"":"":"":"90f5c486e7efe932258610e744506487"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,0) #14

ctr_drbg_validate_nopr:"d3f64c11aa21bb2d12278847547fb11b":"855c0e3a7567730b11e197c136e5c22b1dc7271d4dbe04bcdfd2fc0ef806b3c05b4264ee6c60d526506622ebf6130738dba4bf35c13ce33db19487312ee691fe":"":"":"":"33ed7089ebae738c6a7e6e2390d573e4"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,256)
#0
ctr_drbg_validate_nopr:"132ad1c40afb066620f004f08409c59e":"2e5beadd89b663b3903d3a63c3ab5605bfb1a0045a42430e0220243c51a69f7ff7678c2f8edb7bb4a29b646f3edfaca2463f9defd342da87d22b1b8fdb012fd5":"150deb841d1a4d90e66e85b036d9f5a7efca726b907ae3e8f05e1d1338cdfd32":"fb199beeeaf3939be2a5f9e6ba22f97cdd2c7576e81eccc686facbdf8bb4f2aa":"4293341721f57e4548ce8c003531d38622446c8825904e1b868dcddc626c5164":"66d8f3bfb78186b57136ec2c1602e1ef"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,256) #1
ctr_drbg_validate_nopr:"1c1502ca97c109399a72a77c8d6cc22b":"1d33b1b257a3ae1210fa2099307916a73dd92270769697ea2d7901f56865e3cae1be94b5024d0da3880bce06f0b31231c5a889f8ba3d92a20844b61009db672d":"23eede46eff4a04b08dcc2133e4537b332351f8469630f11b0c8853fb762a4bc":"6fd9f9da108e68aea9d1cecd81c49bcd0e7bedb348890f2248cb31c4277369f7":"76bcc11bd952123f78dd2ba60dd932d49203e418bb832d60b45c083e1e129834":"a1eee46001616f2bf87729895da0d0d1"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,256) #2
ctr_drbg_validate_nopr:"c79c0a1db75e83af258cdf9ead81264d":"5e8cc0fdadc170ed0f5e12f79a6b9e585f9d7c2926c163686a6a724495d88fabcec940d752545cae63f1792dcb966a7325f61997ba8883559ad6f6f8fc09898a":"a2cf6c1c9e4489f504e17f385f08aa82775aa2b0a84abd0b7ee3c6b393d7fd50":"c7529b874e07d4b876196786d510cc038c9e1ab93c461df2474eba484ae6876f":"63c6e7f3548529386c9f47c5aece52ce8454da5db9a807a1b960f7730a61582b":"43b7931e0b3b3769ef8972d0026896a3"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,256) #3
ctr_drbg_validate_nopr:"b44d1dd914e88840bc65a94ee199b3ac":"c3dae1863d323cc78f43ccb3f632fde29130e6b23b843ff5a8d79fddc3c1f92b55cd3dcaf7848d40d189c0de7790bebb889e01be05980dcdf30d2b3333426c50":"41e2fce9b48642a1b9bd1695314adcdd38e1a8afe4891e633c5088c6753438a2":"1eb3f8bbacb0c6b901718bfd7eba29f6f87e1fe056ad442d6d38c1351a684e1f":"85570db773f3f5202967376f91a0a9c09c89cd4eddd58cdc6210335fd5e7acef":"bd53036538d9ed904a49966b5428a2a8"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,256) #4
ctr_drbg_validate_nopr:"5ef97f7af7df5cc6fa94f8428ec7be5c":"be67434ac4d77f0f50ec5bacc8112d1480bd9f20d6b4ea768d9b51bb69c1dffcd8c30e4412127644aaa6fc453e59fb633f6a5a8c2f69e40d1863e35d4d4c0227":"a64195b1e56cf97fd81e99fa1833d191faf62f534c874def4b8bed0ae7195ac7":"353cd3a8d9cd92bce82cd8d1cc198baa9276db478b0cfe50249e30c3042ee9db":"393ab4726f088fdfeb4df752e1b2aec678e41fa60781bc5e914296227d6b3dfc":"24bdc2cad5dccd2309425f11a24c8c39"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,256) #5
ctr_drbg_validate_nopr:"567130da4e7ecc4db0f035d7ecb11878":"cc070df6aa3623f74afd85b59d1bef2b1fcd9c8093362512ff109ebfe992ed75bd58b5ae1561d702b69065eb3cc0bd328ab698d4c6ca274e96d673309b5df5df":"42033054cefa1f20b3443f8ab7d9635ae8f047b833c8529245ba8b4aa07edba3":"72972fb947bff60df291888ddbfd91e698e0c1c26a346b95fc7c5dac596d0073":"af29b6a13602ba9c6b11f8dbdeb6cb52e211f9cd2fc96e63b61e3c1ec631d2ea":"b0849f8317e043271a3fc5f2eaaaaba2"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,256) #6
ctr_drbg_validate_nopr:"2c20ae36f1e74542ed8b0a177b8050aa":"c4bf7a39caf26dc3f61311f54ab3095493c626a988f5abee2826c67a4f4b4d6a02329c99a6bcb5e387fa160741c871acc2929c1cc07f2f0a7ce1619eb7da1ec4":"97c148dd10c3dd72b1eaaafbe37a9310ed15b23872e9f2b62d1feb91ea81ffe3":"23df0c30c68bf2eeb55d273a596f1f54ed916271595b906e4f7793b7a52f2573":"22f120fa09215105116919aaf8eebcb69eccd5da42feb737018a05268bf08e46":"b7c73b9ceea2e6ca0be6a3773cdd6886"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,256) #7
ctr_drbg_validate_nopr:"2076f9e116a2648e1e664b815b1b3674":"979b5aeafe555aeba152ed66e32e30e110df20ee1f227932a72acfb8218aec767941efaefa091c0128dad9b93b06b28fc76e01f275e8ce1c02f0eb567c914f89":"d12fb10b9fa6d2fd0f39cf76294cd44dcbfa80dca7c2f8537c75453d985ef551":"4228a99faf35547a58c1a4d842301dca374f1f13c6fd067b7c1b815863b73158":"a3a7d5f1e2dcf95a90715ec5fd32e7f88c38b0a452b6ccd1f107458db4f74fd6":"8a63a5002a3636b241f0bec14fd9c2ac"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,256) #8
ctr_drbg_validate_nopr:"a71015cf06ddd0a6cd72fa014cf0aee6":"c810cb9db0f169dbc30fda85ccb6d4c40db68d429eeb3653070db7641fbbaba60ef0ff970eaf40887b7e154e2ecd5331de7004689ec604e69927da630a8dd7a7":"5f99f45d8770041703e5a14521c501904fd05ff3340835ac0c41b86442e4939c":"eb7efa6e46ab926ea04c87eb9ce454f5b10717bd9d85305f27d71bea1bc991b3":"cbc80c6171d098fc81023486d327efe2415a0f32e5fa6f6793ce1d0e98783258":"a353f6b350404f3f7b4fb724f84a948a"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,256) #9
ctr_drbg_validate_nopr:"395931837614c322d8488ec6a2c4c919":"831fc8d63592b6ce358c08aeac39d67c3e48b4c2617735b6fe5e9fa44d7aee9d60f2fcf549db239d5bed9c608c94e8f8c23b32901442ac53442127377bdcf205":"eb261c737c0a17c8cb1ae055c143f701b74c96c852e4a76ca3ea045e7efdf5ee":"153276007b3843a897efbf022bd1bcabcf655c7eb8acef9baac710b339ecfd99":"a8a5cb17a2945e5b41ff370cc88ac498389b89b6cd82bb3bbde81c212f7c17d4":"537fc2b73183d2c0c106886937a6609c"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,256) #10
ctr_drbg_validate_nopr:"9a1983859dd6c4cb602970d705952b2b":"68c5cf31f7959ffaa83af9dd55a75ec001befbf835e42a789ac42d39d96128eb6d9b3f07ced15e57e39760390c065fb4425c19ef7184635c18e5ed28256937e1":"e06497a181a5362980579c91d263f630ad4794519a64261ede8b36cf0ac5e713":"714e4fc52aea763e23a1f5b18949ab8fd949f1768560559bccb49d78d51dfab5":"6b6b7f65fd472ad428df2bbb86b85067d0a6f89d9233eea92f5189a9163d0419":"e32af8a81c59dc44540ed8845b447fdb"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,256) #11
ctr_drbg_validate_nopr:"230576e9518fb9a6a8391a84919b0d97":"6193f0e7b33ce19fde922aec9c93f1271ebcdd296d9c8c77029b59afa2064e3159088e07e91c14a4a3dc23b6005dd8ef1425d7d2ae8282a5b30b7498b6754234":"ffaca30a256d18836a0d49bbaad599a28fc7821d71aa91b97158a492d84a6280":"a3da13852d0717afed7c58c52530d2ae047b645a5e7aa8cfabc11478444151ac":"e15fdaeea31c95555fc509d2a266abf78d86ca11aa2f87ce1041142eb9f82bae":"7906f8da1e140345c191dbc2de5ead1b"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,256) #12
ctr_drbg_validate_nopr:"e08a3a33adb4399a9be72fead224155f":"cfbe8b1464b00bb9e0d18b04d2040ed9bd8227411

88812b98a440fbc66ff018ddf6c0ea20c62d01b8237bc7c3da9e3f9fb874fca79a360b4f0f967d8d02083ba":"56f975849197e2eae5a2e6fb445a93c1fadf57280ac27e27c7cbea2cb00c10cc":"0a6d9e2d6e181addab0ea1ee89c65ce557e10fb8e8d43a24cdd27033d3fff507":"823e9400a9f563cc1fa5daf10f4ff1ab8affa18d8371f9cd0e067fcddce8caed":"5ded298f98cffb2e7f5ea97bd50c7e3e"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,0,256) #13
ctr_drbg_validate_nopr:"11c13b917d9f94fd7a008566d8598e89":"f53343a5a455132df3d1b03db39e44d933855b375d7422ad0d07dfdfb352af28946eb29980793456ec8634bf113e75783246bbd05aa8a7cb5886d372fa012f58":"ff1d8d33083023ffbe28f153bddfa9d9f3c221da16f8f20967d2508fa7752b55":"66a98c7d778d798617e1d31d4bdfabf8d381d38b82125838ddf43fb7f5b27dc6":"407c72d7c890c00b249be00a53ae722e5d8033c84b1e1a6a69d4b278ba5db9eb":"67ab88156f20d03b3a1bc363daefc0c6"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,0,256) #14
ctr_drbg_validate_nopr:"7b95343a4ac0f8c8b2645c33757a3146":"3d7e2987860cbcba14a12594e1a394ee754c9a7a65cecc990bc79b5e86e672e12f8c144d843e1abca46b4759a11b3d29f4e219077a8696efadee618f254cb80a":"16297534a79c4ae7493178226b29e42a6f1e0066aeaee8b5af65bcefa2ee3ebb":"b429ee986f16fb35fe2c47c03c0918870b4560f4ec4678f9df471cbd7ca6a887":"2b14d612eb00c7fba0d8e23bf91df91daef6f8e279e0050d5497ddf0f3466c76":"8f72c17405163090fe0bd795b65811c6"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,0) #0
ctr_drbg_validate_nopr:"327290da2e9a19c840de8d33e425efaa5aa7a7afa4e5a812065965478d640f78520cf3c670b098943fec1914d4c8c411":"80bdf18288cb8adb6e3dacb09c553af2e7317c194d37f433eec27e324a0bad752899bda91fd41e5a08acdfd76007aecabc19c95a8bcede310f7320ce97aaad0e":"":"":"":"c26222662ed3a649a1745dee5df4eef0"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,0) #1
ctr_drbg_validate_nopr:"be14f473472db07a43b7f9a517735d7f7ede2aa70dbdb729bc4f578a0dce9d7fe9fd97939cd1ef731262417b5213bd7f":"ac71ff53140c1383eb379e5311e37637af933db494e5e689d065661e9095b8302e4174c392f324fac43695d9381e3cf4626a5347938ed9e21502cbd789cca363":"":"":"":"4bab95f9f05fc36a337b6f2582c2ce98"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,0) #2
ctr_drbg_validate_nopr:"88c31e24f4f859b668946ce73f8600621a70731440762b3c267ceab52a9d77a23d6f70ddba0e46a786697a906ccb18a3":"bf9bf25a949d447274a8c72f1ae51399521f8aca39b1b37bb7b4d5cf3c67d55ef8dbacfb71aa9c5949416e2868b968883e517215bc20292894f8406ab39c1ea1":"":"":"":"841aaa0b171d1526ef365b9201adbff3"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,0) #3
ctr_drbg_validate_nopr:"8545a0de5ea028c8e5976d5b58fa50079b20ba716f0856cc1af7b98537c895f0266b956542d2b8ca661aef5da1f7f8c5":"686f4f9ee74c3402845fbad9353d7dfeff727584d892eb64bd84b764110cbe4ac8581e7e23acb95caf12979983e8947c570264aec292f1c7b756f7184007dcba":"":"":"":"f6d6ae6449b2984df8bcb69584fb16f3"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,0) #4
ctr_drbg_validate_nopr:"d6cd4b4fb9105374605deac7bb49ad792eb225daa560f2a86f66269bf9afc2ea01b6ee6f0eb4926d2f09329df6e90d79":"5d1b8fa0ca2ee127d1bd41423c17b9a8c736715cc2906818e9216dfd81b7637b66c89b772b55ae707c6effa2d9ce7425df26f966646ab613d5599143cf51e5e8":"":"":"":"c36ab451116d733eb4377de3511db5ce"

CTR_DRBG

NIST Validation (AES-256 use df,False,256,128,256,0) #5
ctr_drbg_validate_nopr:"e73ebae0d0834fdff1829ac3d9722fe9f1bc65b5f652fae5f7615af116440e3d5709b5cddd6065d568c246820de46b09":"2026cf7c1b1fe9645ab8759958ac04fb1d8938b9913c3b7f22da81e398b2c00b1921e1d4edb5d21c4531515cb0f9644fe8068685b9fca813176e6780796e8ded":"":"":"":"98d1dce30593de8a8d5b4d956f6c684b"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,0) #6
ctr_drbg_validate_nopr:"a53c1813c06b609eff9ddc77204b085ca985f22170b8ecfcbbf45ea11c45c24fcf25bc33150f9f97ce48244d5beb685c":"1d0dd1a87d59c69f28e118e1083d65f1ee0df31f6308a92dcc47503ec4d20a018d9821c6a7d64385724f0e941231426e028efe6d75e53ff8edf095ef1baf2656":"":"":"":"035cec3a24ba7c44e5c19436c2689a75"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,0) #7
ctr_drbg_validate_nopr:"16d5b8290693a5c40c5a526dd6d653ac54cabb5608d77bb2cb7d6270b96c2fe2de076716ae8cf0a5c781edbde861dc70":"aa82a5ea33439d0c16a1cc13cbae53b169f4d369bcbdae81a9a38129c65ae0ea4f720576c012f8d7eb1c0202003c39d28453a22e502b4949cf5ba23a727721bf":"":"":"":"de4ed9d163d11e9b52470d078df4c869"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,0) #8
ctr_drbg_validate_nopr:"68bfabdbb821cb978527ff18ce37c96c79ad751756551f36b6991981285a68854ec7f72f548c3395ad3ee40410064d4b":"3da9e9518eb1f1b6268e4597f158844ff672ddb414f7ec23fa66d6c86b90a732a7b3016a3387ec3dbed34eb479413d017932ebf9f2a2fea0b35d2bf4e06718f9":"":"":"":"ec4e3e2b6b8763deb17b8611d1fe7953"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,0) #9
ctr_drbg_validate_nopr:"171a74ab694a7d7c2baa3ccf103ad94f11094e07a955ae9ac3bad370f1448753e99b63cc23d1878ab66f94136ec2ecac":"72ebeda7342770d03bc0e531754f946ca5cca684c41f9d089fe9147fad93b6154919c5cb2e6d162fbfde7b9ff0aa590a17993ca6c80bd59eee4134fc2ce944d8":"":"":"":"582ab4f105c3e1fed9593f58fc335fc3"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,0)
#10
ctr_drbg_validate_nopr:"caed30015b34064762591eba9a59f440566a6621832f650572362229e8a38cd0f5d6d322afd8444132056690d6fa5540":"8e27f0dbeae4613bcf0011105f824ed2ecb150a83a0994f8f6607833755216e016fb175e51d42370afe27b11c18477886b530c95bc31bd1c0f8fe00f61fc15a0":"":"":"":"d42787e97147d457f1590c742443ad92"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,0) #11
ctr_drbg_validate_nopr:"c58d62f8145622cd86cfbda66bc26d2ce4c5610cd9cd1c326b99b60355a6fe751783c07f2cc21ba68f1f20ca70f0ad31":"38a8b685e6bbab67824f4cc72995043ea2854f067f2afaec762c9e78ff9d585a25bc63c8d0d075d06d43f3f694733982d26cbe0648b2d0cf8053918b912c303a":"":"":"":"84001709f15a2fd167c161b5d376d86d"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,0) #12
ctr_drbg_validate_nopr:"dc9719050d5257152d8a7d60d3ef1fc5b8cb1700bafc7de863c019f244779c464b6214f21a2f6d0aa3ca282007615ce5":"f188a1ba21b1791ebf8a08d8ba555e49423d9178a561bcc1672539c3a7ba1d856eae9922c4d96c181ed045d6f1d15e855690cdae451edac60f1ca2021f1fec57":"":"":"":"7540fed313c96261cac255bf83b5ae99"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,0) #13
ctr_drbg_validate_nopr:"ff057781af4a4a1eefeb26ab38f82a2efb6f065de290ebf225bd693dfb1f97455b49143bdb430324c9d945c48824f6cc":"0ddd0f4a43a7b54d9abb0928a2242c378db7a95a0b206baa642afe5cd55108f412f1d727fd591bca2c76355aa62aa8638cfa1916739bc66e02b9459ccd0881ba":"":"":"":"8b6e74a94fcac0d2f212d3594213fbb6"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,0) #14
ctr_drbg_validate_nopr:"ef027327e47fc5875c01cb17d798fdc2b27a5c78000727842f8a516f4e8dd34afc167ae145b1e763bebdca51e2f461a7":"128566fe6c5b5595742190519445c25db85ee0ce29371f4cab213400d479d2bfe27655155be0fa237173abb214f0226a2f1770802dd69485adb25e6d837485e1":"":"":"":"76cd1553b2b73d4ef6043a09fb90d679"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,256) #0
ctr_drbg_validate_nopr:"8e1a59210f876d017109cb90c7d5dd669b375d971266b7320ba8db9bd79b373bcc895974460e08eadd07a00ce7bdade9":"23677c04a2d6ab446b7b3c582a8071654d27859441b10799f08b788378b926ca4306e7cb5c0f9f104c607fbf0c379be49426e53bf5637225b551f0cc694d6593":"19e914ffbc6d872be010d66b17874010ec8b036a3d60d7f7dda5accc6962a542":"bd7a0c09e780e0ad783fd708355b8df77b4454c3d606fb8de053bffa5ecf9021":"d284dc2caf6d214f8909efc9a75297bccfc04353c2788a96f8b752749c7fec0c":"129d256e7db6269e5a0a160d2278f305"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,256) #1
ctr_drbg_validate_nopr:"00674e633670c9971be7af789d37d5a4ef567b3ca4766722cd8f67e09d21cbbfa08d43ea1aa259999c6a307ae6347d62":"ec47b029643f85ea19388b6e9de6ab22705b060ae10cee71262027d0bdff5efd7393af619bc6658612fabc78439a0bd5a01255563a96013fa130dd06fd0f5442":"5b92bce3f87645126daa4704fd7df98b880aa07743a57399b985ad1a00b1f2fc":"8199de1338c688234c77262ef35423f4695b277726c76d8b5f426399c14d83b5":"eb95f5a4d8400cec2d4e0f548b6e92636b5e284fb6b61766a1f35bb9cdc5df0a":"9fbe95817578eb272aa9da2f509c2a06"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,256) #2
ctr_drbg_validate_nopr:"2553423c3cb0fae8ca54af56f496e9935d5af4738898f77f789a9bee867dfbc6010c4e5bc68da2b922cdd84eea68e1da":"a9bebd13711c0c22c94b3252654854515a9dc015fe69e688fbac9676b3d77ab67e19b020cd2427ac789ca17f656e499be3ba3ab2075ff95247c6355157eebc79":"e74e45fa28697a06dab08545fde0cc26e7eca31c40aa68ee41c4de402fdcc961":"5aa8abf7062079929d6a131cd3844a5fb6514c07061e25cad67677d867297685":"84819109b2e09b46ba3f5464c34b28ce25a186f0e0fd83fe5fa0ab026c01292a":"3846f3406e49040c48b5cfc9cbc75d1a"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,256) #3
ctr_drbg_validate_nopr:"856f1371454bb9aa06be897dcda9b295817c6eeb865a9acb3a89d145bfe29ce5e1b3b12b714571afdfaca7951cd47e33":"a691b8bf6a407c93a36d18aeced4c75f76d8397d4ecbcd4e8f820cb393186897f05c1ef668b027fc78ba6da9bd554cc31a467d47b5e534b5340c7799383ec05c":"2c81d1e94b33164a177d0183d182fe7d23ef4f88444246464e58bdd0de38d82c":"1b5dae81c96771bea091521c0973c5af76a03e3624160e2511e57ff43a1d32a9":"bf5878e2bd139f8f058f3d834acd771514da6d4c5b9ef84466e5a4e0e4b2eaaf":"6a5ea73aad476ce201e173d4d5a7ffcc"

CTR_DRBG NIST
Validation (AES-256 use df,False,256,128,256,256) #4
ctr_drbg_validate_nopr:"0436075cf8cf62ce623c2301ebd45203c98282611cfa5a12dd7c04525ffa7eb343a607af2f57feb7ce3af97e0abc2285":"1ab9ada5eeebc3fc8e53f358b643476fcfd4dd9f092f21d2bc1c4bb1ffd01a0c5b207aaa09ff76a9cab0aa6ce62b6a65b2650ab448b8bb2e8696a7aa4b6f4e8d":"62f07d1f49e40f7f472985947ac4d8ef2d58216d918f7942b9c70f43daff8972":"37ae758141fbc890ee7e1d0854426b2984fb1c094677e6a61546e9315bab0898":"353d1dd0c8d8656bc418a6a3ace138ecd62819d4e21b8bd87694ea683ec0cc37":"bfee6bb4afc228da981bfe7f0d17578b"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,256) #5
ctr_drbg_validate_nopr:"d004a0893bf326d50ee52e04cb3e64409f204f4e9af780d5dd092d04162d088385b1f243000914c62cba3dadf9827c81":"c36004075f5fd078137ea08de6cb15f71aeb9eca21c891cfdf7a8c0d21790c94ffa93be5fa06beb5e82d9fbf173ef9b29c18511fee2455dbbe61d6b01baf024a":"7d313ada131650c7a506d2c194444ed202d568544caa75bbc60e57a0b74c9a10":"791d60238677ff53150cf7074061eac68335c0a7cec7de43ea63a5df0f312cd8":"6754366

be264deb9e94f39e92ac2894bd93c1d7e1198d39e6eddccb0ea486f4d":"1c29795f03e3c771603293473e347ab4"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,256) #6
ctr_drbg_validate_nopr:"9a8c79b48ada409183f7260aa1415c9ee4e0b662e0fb81b5c56f85d76ed75efac5751dd4de7e7f8b53a36ee0dce2bc9e":"c4d68b76dc0e785823be2da9d339dc900132f12721e8a63ebe92e36d740c5a5e5564c367bff4a52bc70b1c60c86f0bcb7c1d99c414956a259963207184f01246":"04c7060f36569a5d9578c718627fc2695e8d783c0c8aefca2744da6664e67c8c":"1d4b7d587421dea4f7f3e77fcf997607ecfeb6e665a9a184138eb5736b16f516":"8cb8daf9cda230d8d39b829b968aaa5f5d3e3106d8b693227ab1b6201b78a7b8":"faa146098526546927a43fa4a5073e46"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,256) #7
ctr_drbg_validate_nopr:"a0736a5a8b0a394625d8985b05e3a9f277c7ba03b253c0e783359a8c4c086121cb46ea469c7756d5f099f5ee8ed16243":"ea7a046fa1760866bcb37fecf9ade7bcea4444662ea782d6f2820b22a96bab97b4c5adcb0a50ced885121b6b85a5074444b1555d9655f4f6ded31fe15281b30e":"47f3655dd05c42454fad68e330aabca49f27c76ba05ef07b6d77fba41153c0ab":"a5d07da3e399cc51d136096599fcbd9779e839b1fd86f21d7d1e23acd91f9fa7":"150b028b64a988fc1ffdfc9e66b4c8dfe4fcd8538ee976c89923638ebad33802":"6ffdc685169b174ad0dd84cdeed050a7"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,256) #8
ctr_drbg_validate_nopr:"d445a3d9332c8577715c1e93f119521bd31a464db08cdbd73d50080d62d5a48fba4cef2dd097ec749973037e33e8d6fa":"da5f9b2db13d0555846c00da96115036bb75ace66d56fc582d6cd0171e3e23335c5c2b8691e58af8899ed0204316479f849ca6f47309cae571ccb42d3d35c166":"79346394f795f05c5a5199423649b8b5345355ef11eb4239db1c767c68afa70a":"c22810de9987b228c19680eb044da22a08032148a6015f358849d6d608a214b9":"7747d68ca8bcb43931f1edce4f8c9727dd56c1d1d2600ad1fb767eb4fbc7b2d6":"f5c40babbec97cb60ba65200e82d7a68"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,256) #9
ctr_drbg_validate_nopr:"2728be06796e2a77c60a401752cd36e4a051724aa3276a146b4b351017eee79c8257398c612fc1129c0e74ecef455cd3":"d663d2cfcddf40ff61377c3811266d927a5dfc7b73cf549e673e5a15f4056ad1f9733c8ed875ff77928284dc1cdb33accc47971d3626615a45b9a16d9baf426e":"62349efbac4a4747d0e92727c67a6bc7f8404cf746002e7d3eeffb9a9be0bbdc":"381c0cffbdfa61a6af3f11ccd0e543208b584c3f520130e33617564ec7a48cf7":"6974043362f834fd793de07ceebd051599163d50489441005afc9db09a9ab44f":"df7894746c599e02d985b195ca3b4863"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,256) #10
ctr_drbg_validate_nopr:"2b65b56de410ee82e55bd2bf80e6cee356a37c3a3aa7042df45fa750a74e097b071fc18d6eed96523dd4fbb677b8c729":"bf03a6b3e8e23ff53369b971217dc3d3f4c1211329c94847347b3aa77dc7a3e0670381573527844a1ade786f18631944558defffb9a00900ca55f97ec726126b":"59255e5cd2221316c945bd614471df76d5b2f394b8829de82e5c30bc178565e2":"5739bc14f0f2ef9d3393928aee67b0908adaf587650928916d8ae78b0077a3b3":"6b236cf0ee0dba0c92b26c60235d3868715a80c0efbc0c898b6f0b1ace8146e9":"8374b571d7f2d94ce2bdadeb9d815397"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,256) #11
ctr_drbg_validate_nopr:"8756ee2c5e381c7c1dc530748b76a6274ef6583090e555d85210e2356feb2974a8f15119a04e9b481cd3bc557a197b8e":"19705743eaaaa0e8890a0faa2e0df37c820d556c7a45f04d76276f9f9ce2e7c133258ae6d1ba9cdf7745d01745763d18dcd1af2c9e9b0bed2806e60f0f9b636c":"2b4a92b682e9a557466af97b735e2ffdbac3bfc31fd5be2cd212cfbd4b8d690a":"e86504f10317bbeab346f3b9e4b310cbe9fbd81a42054f358eacd08cccab6eff":"19ffad856a6675268cc464ca6fdb8afd0912143e552668528d1484c9a54592cf":"f347fd58aff2999530e258be77591701"

CTR_DRBG

NIST Validation (AES-256 use df,False,256,128,256,256) #12
ctr_drbg_validate_nopr:"f58be57e5035d5c455b17a41ccf7542ffd77f5c009e0a737118ed6c4188f78fcbdbe946bf82e1f
a50fd81691de82dcf3":"f9939592ab2b31d92ac72673da013a588ea17bbf02cfd6e79d79f8296601633d04ceb005110f2
66e6100040ef33194858def8b535314c73caa0e48fc4d2f6e2d":"bb1cb21a316d4b88093cbfc7917d614dca97090cdc8b
b340d864547cb3e1fef6":"7e42d5439d81680c8edf5c571d548699730cfada33b650a4d510172a42b298bb":"e9e3cf18
0f72ba2c1a45d0a94b822943612143e0b642398796b0428ae1af6cf5":"d0c83a4bf3517648b441d411ddcb808c"

CTR_DRBG
NIST Validation (AES-256 use df,False,256,128,256,256) #13
ctr_drbg_validate_nopr:"898064243e44ff67151736ce8bb6f1c759cab4aaca9b87543a1ac984ef955cd5db76c1aa56aff
83f1f6799f18fe531cc":"b8d6be3036eeb5657fb10766354d4be897bd27973b3530270ccc02a08169a2e437b30a3635e
b6ccb310f319257f58d8aa030c8aab616418e0914a46131306a0c":"37572428df5826e6ae5ce95db4ef63f41e908f6852
04a7b64edb9f473c41e45c":"28beda0e0e346b447d32208c6b4c42dcd567acfe1e483fb4a95ea82cb8ce55a5":"7a0fffa5
41d723e16340eeb960b1b9c9aae912477e0ebfac03f8f1a3a8bdc531":"611c9f6fc5193dbe3db96cbcd276168a"

CTR_DRBG NIST Validation (AES-256 use df,False,256,128,256,256) #14
ctr_drbg_validate_nopr:"50de72903b9d99764123ffaa0c721e14ad1ab5c46a34c040f25324ba1d937b8ef10467161fcf
2978c2a680ac5570c6d2":"5c9954fd0143e62c3bf2d5734052e3c9370f7b9d75c70f58fe33b12e3997ee2c8db84f8467a
ffd7cfd9a9e7ec60da6f31bf9bf32aedf644e4934bd1fc916bc8d":"d5dc4c9fc7171fcbfdaead558a565ffd55d245a58b22a
d1666ee05131e33f49e":"ea3114e92e6a19f53b207a0a54cd363a6d053fed0a827f92556f0a8580f7a342":"53686f069b
455af4692888d11fac15cf7b4bd38e198de4e62b7098f875198a75":"9fb0df053e0345e5640aa97fedef50a6"

CTR_DRBG
entropy usage
ctr_drbg_entropy_usage:

CTR_DRBG write/update seed file
ctr_drbg_seed_file:"data_files/ctr_drbg_seed":0

CTR_DRBG write/update seed file
ctr_drbg_seed_file:"no_such_dir/file":MBEDTLS_ERR_CTR_DRBG_FILE_IO_ERROR

CTR_DRBG Special Behaviours
ctr_drbg_special_behaviours:

CTR_DRBG self test
ctr_drbg_selftest:
-----BEGIN CERTIFICATE-----
MIIDCjCCAfKgAwIBAgIBATANBgkqhkiG9w0BAQsFADAmMSQwIgYDVQQDExtUZXN0
IGludGVybWVkaWF0ZSBtYXhwYXRoIDIwHhcNMDEwMTAxMDAwMDAwWhcNMzAxMjMx
MjM1OTU5WjAcMRowGAYDVQQDExFUZXN0IExlYWYgNCB2YWxpZDCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAJEq4FhQ+JWENERf895iWY59ZYDQZIZwj9IX
Iib/3raDDd2wgfrnPH6NMMQ0NmXG80wENKgTZ4ybwCdarJWQPW6CASpk/CUosYov
9V0w1iNxOWjr19YepVuuqVbCMy5tDQH9FSZ9sS8NGL/IXym8I3DXgH5uxgsCQfLJ
I3pDCifPnuqT+GR8Zq5zqNJFJQoPMPESs2erGCcV9RE3pFjxFEl67HEP2Eo6Ts4y
w6YdZTuIFRKwYXSYCaSc56pK0QYke3/4SK6QFd8DlG7X68ayG+RVzjPa7f7L1kUa
8yFBpwb6NOFmfikBz7DJ/vcfIvv7bnjoNSi37NdIVtEVrE0I5jkCAwEAAaNNMEsw
CQYDVR0TBAIwADAdBgNVHQ4EFgQUjga9VOIeT2Mjqhnv4CYMFpOxX3swHwYDVR0j

BBgwFoAUwjdrwy2NbXHp088kZpUuEwXtsYowDQYJKoZIhvcNAQELBQADggEBADdp
VpPr4AzE7ecrhclQKGjPa7leaorYuevjTLWsieY17mVQhlMX1itTNXlPBUfPAsOd
O7LUgY0yZOnV7l8TbfGal8pIF+acgFLgqM5A6z8ngChMi6iKEZChDVffAVHJs3e/
WUm7VeFY8Mvwnay3iHj2trC7XQX2SZCovXYfNP3bVyqIaDNqt6SPY1skouWpmmUn
ISzcyH6EU/CegFjHJyXxrsIW9Nv2mDejrmcR0EJOmEAfWUgonfemeX93xkwZHW2s
lZ8/e6rTPPSGdhY/b4VRu6o1FpLcPLGZSgPwYBNVYtgT4WsoT0xUvm6Y1WipiZda
B/bpiL8l4GSVtTw1Jko=
-----END
CERTIFICATE-----
AES-GCM NIST Validation (AES-256,128,0,0,128) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"fb8094dd2eddb3d8004bb79134023ca2be4de9b668a9e4608abdf2130e8becb8":"":"491a14e13b591cf2f39da96b6882b5e5":"":"":128:"80883f2c925434a5edfcefd5b123d520":0

AES-GCM NIST Validation (AES-256,128,0,0,128) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"725313f4cb3f6a0d29cefc174b7e4f43cef11b761ef75e1995cb64c1306795f1":"":"27d1ed08aba23d79fc49ad8d92a2a0ea":"":"":128:"d5d6637ba35ef2ad88e9725f938d3d2d":0

AES-GCM NIST Validation (AES-256,128,0,0,128) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"4e766584ce0e885e1bba1327e5335796de0831a40f74a5cec178081dd15bfd10":"":"cece0dea024ff47851af0500d146cbfe":"":"":128:"1abe16eeab56bd0fb1ab909b8d528771":0

AES-GCM NIST Validation (AES-256,128,0,0,120) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"ce7f2207f83a952451e714ba3807ddb3ed67c2739a628980411aa68366b1f2f5":"":"652fd951ace288db397020687135a5d1":"":"":120:"985227b14de16722987a3d34976442":0

AES-GCM
NIST Validation (AES-256,128,0,0,120) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"855f8fa4ec6a1206173509d504d0b29dfbfbfa9aa528254b189cd72e6ebc1c1f":"":"1ad1507e6463e4e2e1a63155ac0e638f":"":"":120:"693146a8b833f324c1d4cbeeb8c146":0

AES-GCM NIST Validation (AES-256,128,0,0,120) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"ef8dd1294a85dd39e366f65e1076d53e046188c06c96b2c9e84ebc81f5c9f550":"":"9698a07447552d1a4ecd2b4c47858f06":"":"":120:"b00590cac6e398eeb3dcb98abe1912":0

AES-GCM NIST Validation (AES-256,128,0,0,112) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"25896e587570ff1823639e1e51e9c89192d551b573dd747e7c0c1c10916ece4c":"":"f0516457c09c372c358064eb6b470146":"":"":112:"5a7cadec600a180e696d946425b0":0

AES-GCM NIST Validation (AES-256,128,0,0,112) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"02fc9cfffbe72e7954182993088e09d24ea8cad91a8ca9a336d

9f1fe4156486d":"":"0e189e162e097eb2060b30c46d9afa70":"":"":112:"7d3d5cc55e6182ec5413ef622d4f":0

AES-GCM
NIST Validation (AES-256,128,0,0,112) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"f24e3d631d8961d3d4b9912d4fa7a317db837a7b81cd52f90c703a4835c632e2":"":"510740bfa2562ce99ca3839229145a46":"":"":112:"1402ddc1854e5adb33664be85ad1":0

AES-GCM NIST Validation (AES-256,128,0,0,104) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"720ab5aceb80ff1f864379add9b0d63607227f7c3f58425dd6ec3d4cea3fe2ea":"":"58f2317afb64d894243c192ef5191300":"":"":104:"e8e772402cc6bfd96a140b24c1":0

AES-GCM NIST Validation (AES-256,128,0,0,104) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"f57dd16fa92a8f8c09d8f13cb5b6633a43b8762e90c670232f55949cdfdf700c":"":"3b7c14ee357b3c6b0dc09e3209ab69f2":"":"":104:"43e609664e48ad1f5478087f24":0

AES-GCM NIST Validation (AES-256,128,0,0,104) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"87c17ab919a4bc0d50343c0bb282a969283c2ada25f9a96d2858c7f89bc5139a":"":"02813d3faf30d3e186d119e89fe36574":"":"":104:"d1a1f82a8462c783b15c92b57e":0

AES-GCM
NIST Validation (AES-256,128,0,0,96) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"dd8d5b6c5c938c905c17eab9f5ab7cd68d27f3f09d75177119010d070b91e646":"":"1df1c3ad363c973bffe29975574ffdf6":"":"":96:"749ac7ffda825fc973475b83":0

AES-GCM NIST Validation (AES-256,128,0,0,96) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"4d60a14cb789099c77b8991e7b0b40f787d3458f448501e8108e4d76110f94ef":"":"ca6b3485eb5dcd9dbfa7cffcdb22daa5":"":"":96:"3f868b6510d64098adc1d640":0

AES-GCM NIST Validation (AES-256,128,0,0,96) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"405b690717de993ad945d80159c2800848060de0b7d2b277efd0350a99ba609a":"":"63730acb957869f0c091f22d964cc6a3":"":"":96:"739688362337d61dab2591f0":0

AES-GCM NIST Validation (AES-256,128,0,0,64)
#0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"ab5563a387e72d7d10468c99df590e1de25ec10363aa90d1448a9ffcd1de6867":"":"c511406701bad20a2fa29b1e76924d2f":"":"":64:"390291ed142ba760":0

AES-GCM NIST Validation (AES-256,128,0,0,64) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"abef7c24daaa21f308a5af03df936ba3f70aa525190af0d959d

6e50d836f4624":"":"e9f15950130b9524e2b09f77be39109a":"":"":64:"db2fb2b004bc8dc4":0

AES-GCM NIST Validation (AES-256,128,0,0,64) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"6ca630b0b6779a8de7a19e5279eac94bf29f76f8b0cf8ecf8f1
1c4f8eb04aa0d":"":"7373befc2c8007f42eef47be1086842f":"":"":64:"e2b8620bcc7472a8":0

AES-GCM NIST Validation (AES-256,128,0,0,32) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"acea7818a71df2c9840aef1c10ecbe2bac7e92216388416a2f3
6119a0745d883":"":"6d46aa39fb5a6117e9adf7ee72bc50ff":"":"":32:"fd5ff17b":0

AES-GCM NIST Validation (AES-256,128,0,0,32)
#1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"b301036d4b2b28b8a4502925986861eba2b67c24cb0c79c63
fd62195d9b67506":"":"bb6f398e5aed51590e3df02f5419e44d":"":"":32:"47f3a906":0

AES-GCM NIST Validation (AES-256,128,0,0,32) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"89576d2aac554c8982c7df0053be9ab19f4bd80ba9f3dd433c
1c054d68e68795":"":"aedbd482a401a7c12d4755077c8dd26e":"":"":32:"506fa18d":0

AES-GCM NIST Validation (AES-256,128,0,1024,128) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"43c9e209da3c1971d986a45b92f2fa0d2d155183730d21d71e
d8e2284ec308e3":"":"78bef655dfd8990b04d2a25678d7086d":"9d8c6734546797c581b9b1d0d4f05b27fe0539bd016
55d2d1a8a1489cdf804228753d77272bf6ded19d47a6abd6281ea9591d4bcc1be222305fdf689c5faa4c11331cffbf4221
5469b81f61b40415d81cc37161e5c0258a67642b9b8ac627d6e39f43e485e1ff522ac742a07defa3569aeb59990cb44c4
f3d952f8119ff1111d":"":128:"f15ddf938bbf52c2977adabaf4120de8":0

AES-GCM NIST Validation
(AES-256,128,0,1024,128) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"fbe2d52b7f50bf23a16ff8cd864215034fdfbf4d1506ca3c1ffb
015653efe33a":"":"b155f8ab1a8c0327789cfb8310051f19":"ed8d14adf1c362bbaf0d569c8083278e8225f883d75d23
7a4abcd775a49780603e50c00a1b5b5946c085e57a749b4946f6aca96eda04ac9944a7d3d47adc88326ed30a34d879dd
02fb88182f9e2deefaeee1c306b897539fa9075bda03ba07b4ffff71ce732ef3c4befac0f18c85a0652d34524ccb1a4747a
b8f72ed1c24d8fc":"":128:"c5fe27ca90e5c8b321cc391ee7f1f796":0

AES-GCM NIST Validation (AES-256,128,0,1024,128) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"8e888721514fd01fb67513cb56bfd29af67a9ce525e3e697af4
7450f02053161":"":"9f6bd4a93e4f3f2f5f4a7c2c5b4790bf":"867d50923967535ce6f00395930083523c22f373cfb6c8
817764f5623cd60b555572404e54f2fe7083ef32b9a4593a1f70a736d6e8fe61b77def51f3b1d8f679d3a8d50d0aad49e5
1ec1eb4d4a25f13d14f3e5253555c73eac759e484c6131cc868b46c18b26acd040c3e1cb27afecba7b7fc3f5ff4883f4eaf
c26c7f3084751":"":128:"ea269094330b6926627889fcdb06aab4":0

AES-GCM
NIST Validation (AES-256,128,0,1024,120) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"d8f82b07e7319ca607c9aa0352070ca883dd7b32af370a774f63b0270f44835a":"":"e89e4484497cb728f86585d8918b7fae":"42340d96e1852de3ed5e30eb4a05e1fb222480b450e2bf4e2cf0fb2a525eb6602ef43a896adc5c52ea5381c642b2175691c014e7a6dae91fa6ff5b95c18a2dd2e8838d3abd46ace0b305f3f22d30a0bd82a81bbf6753362b54b0624c76c0d753e30eb636365f0df7e1bf8bf130cf36062ec23f58a3f7ed0ae7bfbbd68460cd76":"":120:"b234b28917372374e7f304f1462b49":0

AES-GCM NIST Validation (AES-256,128,0,1024,120) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"b49b04a54a08d28b077ea54c18bfa53e916723e91453b47f88e399046b9b4dcc":"":"6276c577c530f91b434ce5719e1c59de":"6b73f996c49e368fc4d21816153aefb081509f9dc0916dbe4fdf77f39867a2bd617b8a75f39f515b1bc1454009d5247efcd90ba0d4a6743c6f12a929b666584f3b55254c32e2bab2321f94fa843dc5124c341dd509788a158191ee141eb0bc4e1b96f6987bafe664a0f9ac6d85c59cee9564a27bcc37dffae80c57fbf7e748ce":"":120:"69dd5bdeb15fdbc3a70c44b150f70e":0

AES-GCM
NIST Validation (AES-256,128,0,1024,120) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"398bb37bb991898c7dad7bf5930dbad20d121f68d5ec6c56ffe66f23c0c37f8e":"":"0c3bd55b54c1221b0cf25d88ea4dfe24":"4c48b929f31180e697ea6199cd96c47cecc95c9ed4c442d6a23ca3a23d4b4833601ac4bbcdbc333cd1b3a0cd90338e1c88ef8561fed7ad0f4f54120b76281958995c95e4c9daabff75d71e2d5770420211c341c6b062b6c8b31b8fe8990588fbad1e651a49b0badd9a8d8042206337a1f2aa980b3ba3b5ee8e3396a2b9150a34":"":120:"8528950bd5371681a78176ae1ea5dc":0

AES-GCM NIST Validation (AES-256,128,0,1024,112) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"8e8f7c317b22dea8eabe7eaa87413a98ff56570720985b6743a5f9af56387cca":"":"3a9a5a839045723afdfb2d5df968bfcb":"a87d95f8f47e45a1c7c5c58d16055b52b3256c52713fd092bcd6cbc44e2c84669f23ca2a19e34163ee297f592f6054dbc88863a896c2217e93a660d55a6cd9588a7275d05649940d96815c7ddfa5fc4394c75349f05f1bcaff804095783726c0eceb79833a48cefd346b223f4e5401789684e5caeda187a323962a1f32f63f02":"":112:"faad6a9731430e148ace27214e68":0

AES-GCM
NIST Validation (AES-256,128,0,1024,112) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"67c95e57197f0e0bbaaa866d337fcc37f3a10dc55a059f5ea498de204d2fff61":"":"5f171d203c653a316cac43df99f4033a":"84f281b388ca18bc97323657a723a562607312347 20b02b6dde00ea134bd84a1893bec38af80214c4da01b93958ab00f3b648c975371e565d5b6bf2a8f63c0f3cfcd557c9f63574390b6ae533085aca51fa9d46cd2478b7648b6dcbbac7e61197a425778debe351ac2110ba510a17e2c351ba75d5a755ef547cf9acc54650222":"":112:"9ea9c716e06a274d15a3595a0c41":0

AES-GCM NIST Validation (AES-256,128,0,1024,112) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"9143f00e31c72bd9fced31585d047f67f1004e6244c3d9c10c8ae005feeabc84":"":"e49cd6af9a2f0da2a7198317da92ab2f":"ab9193a155140d265aabfe2dd5efca7d3fa6129498532bccd77f09fa1a480702620b3ab53df91b01262122f1a6fc387b5fc55dadfcdb99ada83d4a5b0666c8526de309f41eb54d6

9b52595c43550a6bf7b4b8f0e0c48311b521762eaa567744c4c4704dd977f84068b59db98a67e33cc65302ba59360d60
0a22138c5ad3317f3":"":112:"8293e361fe0308a067f89aea393f":0

AES-GCM
NIST Validation (AES-256,128,0,1024,104) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"d0ba180075c373116bb037907b512add00ba9a4693a8ecc14
ca0d79adada90e3":"":"5c1501b19cce5404dccc9217ac8253b7":"3a161605ec0055c479dd48cdaeed5981b8b60fb7b7
781cc4e580218c7014c3060a9f706e6e16cf4021e4d38deb512534b484ff23b701975bdf901146ccaece9c3ffbbeeb172c
fb64a915ae0dbe7a082b9077776a387b58559a881b9b79b90aa28ad1ac0f2bece314169a2f79ea4c08389f7f7dd10ee2d
9a844fee79e7bf38bcf":"":104:"0541262fddfd5d01ff0f3c2fb4":0

AES-GCM NIST Validation (AES-256,128,0,1024,104) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"c975c7e59133c231d1b84c696761c413ba20aff7fb7d854c69
47e65db3cc57b4":"":"d8fedda4cccaf6b0818edcfa7b1f03fa":"cb4cc9171367d6422abfaf2b4452da267eb9ccf1c4c97d
21a0a125de486997832d16c7e412cb109eb9ac90c81dfe1a1dd9f79af7a14e91669b47f94e07d4e9bd645d9daa703b493
179ca05ddd45433def98cf499ff11849cc88b58befbdd388728632469d8b28df4451fc671f4a3d69526a80c2e53e4fdee6
300d27d97baf5f4":"":104:"77ac205d959ec10ae8cee13eed":0

AES-GCM
NIST Validation (AES-256,128,0,1024,104) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"a86ec688222c50c07274ed2d2c8ae6f883e25f8f95d404a753
8fd83224199327":"":"99c73fdb8f97f225f7a17cf79c011112":"cf5f707de0357262c0997fa3ebfe6e07192df8db5f029e
418989e85e6b71e186b00c612ecedbfe3c847e58081847f39697337ae7c815d2cd0263986d06bf3a5d2db4e986dbe690
71fd4b80a580f5a2cf734fc56c6d70202ea3494f67539797252d87cd7646296932959c99797a0446532f264d3089dd5f4
bcceaaa7289a54380":"":104:"c2093ad4705e613b09eee74057":0

AES-GCM NIST Validation (AES-256,128,0,1024,96) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"d3981f0aa1ed8cb369d9b0d7b0e529ec6089ff2d226c542885
b1bff55276e891":"":"7331f91bd1a67c21c9dd336a2a922839":"406d9cf45fc8618d564154241dc9c006ecdcd847406e
5a6e7127ac96e7bb93f4c339ff612c514b6f66df95a0845035d7535212a2aaeeb0ee512d1f4375c9a527e4e499389c2d7f
7f7439c913ea91580e7303767b989c4d619df7888baf789efd489b08eda223f27da5e177cd704c638f5fc8bf1fecfcd1cab
4f4adfbc9d1d8ba":"":96:"dbb7ec852c692c9a0e1a5acd":0

AES-GCM
NIST Validation (AES-256,128,0,1024,96) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"8436967f97c59ca73b760b73c6e088d1da4e76b712188ab47
81d8d849505ae47":"":"9401dd0998914645668d06d518bfe7d7":"a5f40906177417097c19a0a21dbb457a694e17314
1837f695b09c8eb58ac2ce28aace4e59275b6266da9369a9905b389e968aefc64d78c7e1d2f034ef413d3458edcb955f5
cd7971c28cd67dc9901ef3a2abc6121704bb5ecd87a6568d0506abbc87a2f10205dc8eb0cd1b5109158d0e743c2c3a34
2d60b8d55bbcb8d8507ed1":"":96:"dd6d988d352decc4e70375d8":0

AES-GCM NIST Validation (AES-256,128,0,1024,96) #2
depends_on:MBEDTLS_AES_C

gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"ce6b846bcedc6ae747e66e72cd9f7664e6cad9627ba5f1f1923f3d3a6ed590d1":"":"ac865ff8a6255e501b347a6650510d05":"1658b9f8469af1dfa60458cf8107db1edd1e4bba70a0bd23e13e1bba0d397abf51af8348f983fcdfcc8315ef1ffc9a26371377c62ddba08363bd2bf0ff7d0c3b603fad10be24ecee97b36d2255a8b2efc63f037123cef4bb4fe384aa0c58548b2f317c36ef3ef204b24769de6ba3e9d89e159e2bf1f9d79aeb3eb80c42eb255e":"":96:"7ee87acd138c558455fff063":0

AES-GCM
NIST Validation (AES-256,128,0,1024,64) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"0038ecf1407bbf0d73afa5e010769b71e8649c4249345dcf923ef9da0254c6af":"":"74c6b98fc6ced3a59bd9c42d31d71095":"467f483c71c3404fe7f09d6f6b6b64c3b7613a0dd32470cf24bc590d3994a48f3e8cd5dc19ea8ca7d5366ad7c5ad31cc9612dafedaea109dde2aedfe5fc2a0db2c903dd1dc1a13949720a10babf37fba5a0ed7cb5f3dc9eb5a4d8331f218e98763e7794b3e63705d414ef332160b0b1799f1ff5cbe129a75e5c4e0a4ed35e382":"":64:"62fe088d9129450b":0

AES-GCM NIST Validation (AES-256,128,0,1024,64) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"19fc4c22151ee8515036c38bc5926c0e0bbd93db5d0fc522b2a6bf6298fed391":"":"9547f056c6fb9ef72b908f527cb500c1":"511b15c25b2a324159e71c3b8e47f52d3e71e5bc35e774c39067250f4494c9c4eb184ecbe8638de9418672d9ae2c6a0e7f54c017879ffb2a371de1639693d654a43cb86e94a7350508490191790d1265b99e7b3253838b302aae33590949a8761a3bb2aeb1ba798cddeb00a53daad05a33389d4a19269d65116a84f12dba5830":"":64:"04623912bb70810e":0

AES-GCM
NIST Validation (AES-256,128,0,1024,64) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"3b5d3b1920b5a105b148153ae1f1027c6d48bc99640ea853f5955fed4eb3d625":"":"9a4091c2eb7e88759bd9169fee303485":"aa680d07143ba49a9099d555105fc3cfcb898cec11ade96776dc9778cc50fe972e1e83c52c837b71e27f81d1577f9bd09afe2260dfd9a5d9dfbd3b8b09a346a2ab48647f5dd2ff43700aecce7fa6f4aeea6ea01b2463c4e82ec116e4d92b309c5879fb4e2ca820d0183a2057ae4ad96f38a7d50643a835511aedd0442b290be3":"":64:"033bfee6b228d59b":0

AES-GCM NIST Validation (AES-256,128,0,1024,32) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"f6c4ad8e27764157789252f4bc4a04145cb9721955330a2f6a2a3b65cacf22bc":"":"3de136cbd75061c888226efab136849d":"0f6951c127d6bc8970e2ad2799e26c7fb9ca31d223155f88374984b5660626c83276ffa6c160f75e0e1bcfa96616188f3945b15fc1b82a4e0ee44000a684b3c3840465aebe051208379ef3afe9f569ee94973d15f0a40c6f564fa4ba11d6e33cf8ae17854a9e12360a2b8495e2cceec463f5e3705c74069ba37ba6d725f458c0":"":32:"f658c689":0

AES-GCM
NIST Validation (AES-256,128,0,1024,32) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"30cd99fed9706c409e366d47fefc191f79bcc47a28be78f9890fd90d4864eb85":"":"8c7ce34691503bf14c776f8809f24e61":"4b6b10c2e2905ab356769b6453dd160a08e8623b0878fcc1c1d64822f0aea1f4f5b4698ded5d23ebafa11bc1e4ce9e5cd7d7c7b13de02d11a945ba8361b102ba49cdcfd6a416e3db774cd7bda024fccd1ad3087560dc15bbfe9b1a5c6c71fae17a329f104f6c2cba7eb6a7459535ca328146d0ccc0a9bd28a3d1c961947a3876":"":32:"7777c224":0

AES-GCM NIST Validation (AES-256,128,0,1024,32) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"9472f2452933dcfac4bb22831ce83c6a1ddf25ef8d2d3ba59d72b0d173a986e8":"":"18fb2c34b0955d712960009617d300ef":"d283dd75cd4689c266c8e0b4b6586278aa2583c7c41bf12bd1cfdef21d349acbbabc0a2204dc4130f922949206c4fbdce3786ab8614e32908838a13b6990453abf14b84f5812e6093644accdd35f7ad611ea15aefae28b3cf1fc5da410bcea4f0a50d377fdcceffe488805bc5a71fab019b12fa8725d6e7c91e6faf12fbaf493":"":32:"c53b16a1":0

AES-GCM
NIST Validation (AES-256,128,1024,0,128) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"e06d5319210f4107ea7267fa2e8183fcbf74fd3b0579b856577177d9cb307d42":"2b9179d21cb884581b0e4f462455167f1f7899717245d4aed3d8db5983dacccebfc2130a20c284563bea5997cc0438c83d8fa7bb9e3588efed285a0fcc31456dc9a3122b97bb22f7edc36973475925828c323565e417ec95190db63b21881016b5332f2e400bb4724c86a8ee0247149370ee5412f743dc6bf7ca5bcc31afa0f":"f2b0564705430bc672964b049115e122":"":"3fa342a76cb5d501e6a6fade14aab54a76620e4ea2287147d4ca2b9d62d2a643591e5df570ef474ee88ad22401c1059e3130a904e9bf359c4a6151ff2f3e4f78ef27a67d527da8e448b0ef5cdcfec85f3525e35f8d024540387e4cdcb1018c281a1af7d4a3688a0fec4d9f473c816f7d4c4c369f70d7dfe8f1b7fa4f581098a1":128:"18f186ed1ee1f4f8b29db495587d0ab0":0

AES-GCM
NIST Validation (AES-256,128,1024,0,128) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"0dfa834e98b6c51ee925dd9edc9be72c209ddcd9099ded57b533f2236895a229":"7f4e4f11091bf51976c0fc71ecbcd0985cdad2135549c818c09567801d8a9a42c719aab7dc2cb58a10b5067d14c52cabe6bb9b939e7b9cd395eaf10ba6a53fd2e6446e1e501440134e04e662ef7ebb1c9c78bbd3fd7cb9de8b985418be1b43ebb5d7902ccb4c299c325c8a7cc1de9174f544bc60828c1eebad49287caa4108a0":"a101b13b238cfac6964fd6a43daea5a7":"":"bc60d2047fd8712144e95cb8de1ffd9f13de7fda995f845b1a4246a4403f61ca896bd635a1570d2eb5b8740d365225c3310bf8cea3f5597826c65876b0cbcfa0e2181575be8e4dd222d236d8a8064a10a56262056906c1ac3c4e7100a92f3f00dab5a9ba139c72519b136d387da71fefe2564d9f1aa85b206a205267b4cfa538":128:"c4cc1dbd1b7ff2e36f9f9f64e2385b9e":0

AES-GCM NIST Validation (AES-256,128,1024,0,128) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"ce59144b114ac5587a7a8079dc0e26f1b203338bb3e4b1d1d987bddc24150a82":"bc7aa1b735a5f465cffeccd8dd4b0a33a571e9f006dc63b2a6f4df272a673bb2cc00e603248ab6be5627eebc10934fe4d1dc5cd120a475936eefa2c7bddea9f36c6c794d2c6bd2594094e56cac12d8f03e38f222a7ee4fc6c2adffe71c9c13003e301c31ff3a0405dde89bb213044d41782c4bb4eb3c262595d1c0e00522047c":"fdc5a40677110737febae4465b1a76cc":"":"084c31c8aef8c089867f6e0ce6e0aadafa3016c33c00ca520f28d45aac8f4d02a519b8ebafd13b9606ab9db4f2572f396091bc5a1d9910119ca662d476c2d875a4ab62d31ff5f875678f25a4775fa7fc85b1a3d442fb2c5047a3d349d56d85f85f172965e6477439045849a0b58014d9d442e2cae74709ed8594f0ec119d1d39":128:"4c39e0d17030a5f06ecd5f4c26e79b31":0

AES-GCM
NIST Validation (AES-256,128,1024,0,120) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"e7a6b459a5370ceec4d429bba9472a49db07697dc66dbc2f29

4d3e62ffc8aac1":"cb959e5611a636317feb5265d33b315c2f5af64159029f0032e338babbdb0a525ba6b92cb3be7db9f0077561e6cffe1247bad32dea8918f562dc3cd83225cdbcaed652b87c62fea8eff153638a3a14ef9f9a88bcc8c9a6b65fa9dcc53f63d1b14fb9bb0baf17e7bfb95690c25cca2c3097497e41f7e2299a8518d5d1c5f6264e":"92468d42ad377affa7e808d95d8c673a":"":"599dbc47e2f2e3b06b641c510b238417b01869f0e7d08619752f6d9f4b08585731deaeb439ff26e02d7e51b45ca5e3d4a779fe4cfc9572d1d6407f98de69a8fca60bf01d1a769130bb38a67933a2be3aa3ea1470d8f32a34dc863dc800feb7ef71588edd9489bd59a23685ff5358f9b562fc0bbad9e11db7a6fedbd79225539d":120:"e853262ed43e4d40fea6f3835d4381":0

AES-GCM
NIST Validation (AES-256,128,1024,0,120) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"9818904a99e3d80c95dc71a16483ade1b9b8e7df638ce6a4c1d709a24416cbe9":"2c073cdc11a8d58fb55e1dadbbc0372dde86c387fa99c9249bd04cb2f2d239de01bec8c8771a9fb33664ee06ea81c37a824525664054173b63a2894d8d7ffc60b9e93052802478a189be5835d979a28ce7025b219add0622f97c9bcf3ecf629b56408ed002a141061320400409345e94a7a7e3906611305f96f2abc9d62cc435":"96a301ab6bc0309be9735bd21cc9e10d":"":"4876e449b0cac09a37bb7e4b8da238f4c699af9714ec4fcf21a07c5aee8783311a13149d837a949c594a472dda01e8b6c064755b6328e3ef8d6063f8d8f19cfda3147b563b0f5fb8556ace49cb0f872822a63b06f261b6970f7c18be19372a852beadf02288c0b4079587c0f8eab1858eeec11c6ba8d64448282068fddd8a63d":120:"e1e8b62ce427e5192348b1f09183c9":0

AES-GCM
NIST Validation (AES-256,128,1024,0,120) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"9b34f137e3f37addad8a6573b8b6dac9a29e97db53c0a7610f37c72a0efaebfa":"c1e09c432c68a2c119aeb3b19c21180e3c8e428e12033f416a92862036f5e8a39a8893b10fe5476e388d079143ee0b79b183a3400db779cfbf1467d69887306b124a8578c173cd5308d4448eefcf1d57f117eb12bc28bd1d0ff5c3702139655197d7305bda70181c85376e1a90fb2c5b036d9ea5d318d3219132ea6c5edf7b7d":"50dddb2ebe4f8763509a63d07322277e":"":"793e1b06e1593b8c0ba13a38ff23afaa6007482262bc2d0de9fb910f349eff88d3dd05d56eb9a089eed801eae851676b7a401991b72bf45ac005c89e906a37ed7231df4aeeeb1fcf206ca1311117e7e7348faf1d58acc69c5702f802287083d3ed9e16cf87adcdfa1bb0c21c40c2102fd0def91985f92285e6ea1cdd550e7f50":120:"b3c6ae17274faaca657dcb172dc1fb":0

AES-GCM
NIST Validation (AES-256,128,1024,0,112) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"66b40e2e671bdf244b45644d1a5adc63011b32156ba9f5e03dffacc1a9165061":"985546ee12ba89d95988ad8a4153c4f9d3c91c0e3633a95b4f9b588bba0032006c93210514357c91d574b436da13dc9f68194a981e7b65eb79e56be9cf1dabfdf531407727c034a3c7743bb22aa02b26f159c2eff3c7ed52027de2e8b8b2fefb72c04fbf20a1ffe10d6dda790a9812cdbe9f2ed6706d7a2639e851a42870efb8":"4e090871e889b4be36db5e1df1ea283d":"":"f93eebffeddfd16b4618b893d57b459b704b894b38a5eaf6cce54026c80090be8328e12261e1b10e81c73ac8261c2982bb25603c12f5ffff5c70b2199515c17200db2d950a3f2064d7b362607adbf3686f27420ec15e18467e86faa1efa946a73c8888b8fdc825742b8fbec6e48cdabbb45f3cd2b6b6e536b6fbf3429aebe934":112:"ed88c856c41cac49f4767909ac79":0

AES-GCM NIST Validation (AES-256,128,1024,0,112) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"18c5105a9651144ce965b4270398b982120b885850114571ef8e2cbc5d2f5e04":"00c5ea3d91248bfe30c5a6d26dbdf0609f977afcfa842b603c1061b2a473c9a79b421b2509550309

e4be9c5015c51c6def9ee68c242f6e206b3027ce8e58b7ab96aaa50ced1d78c2dfcbc2589575bec2ce3b6a5066276fe7dc
a4f1118808d1e5cac062667053c15350289da03cd073377c2d66c01e3098ed01b75788c7e1f9e7":"a3a5f82748acc887
e33328fd7f4ce1fd":"":"d91ed6886a269dc1eb0745dc4b97fc54cbea5e6857d10a303a3caf828b4e0e20bb742bca17021
b7852d09a6d7d3a56ad82298c15a2082fed0e0e326bb16dd677ee262ead93a24147de3c07eb8a95b108abf17357155f1
de79171689407b6545c9fdf8ab4486576490430c0e043e21e7c40ce88e752cb006cb3c59479a7e56cf7":112:"add4e08
6d612a119c6aae46ba9e5":0

AES-GCM
NIST Validation (AES-256,128,1024,0,112) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"4667cabeb3a644e371cbbe9195413daab025cc6efc12298bfa
ea0dd9bc028f9f":"9772ec47f3cd26f091bf117e085f2394db258c2c460dc3b1402edcb60a8f70517f82aa669607b78c2
ad79c662c3b376cee1b9f34c4ec5d15319c33de78a440e7f2a4108c3c9da51604adde2025ff1dc336c49279c13a715393
1df675df0e78f17a4d72973311af74fe755c85c7869baf3896bb738925942dc67f1b6e690c9d48":"7e8927c69951d9014
94539ab95ac5906":"":"5d62fa69cfbfdec30193408dad15cf983ad707ee921068b817676eca9f70f9ca4623a8c113df5fb
a86131415f4ec546c7f1a94ff9d02cb8ddcf421c7cc85ed87ce712fcd8d5f45460749ced0d900fe0368c59b1c082bd5811
c1a648a51768d5e4bfbc23cada3791f289d8b61fd494398be1ad9ee9ff471abb547000ac2c1a5d1":112:"0ae6bd5e8c25
d1585e4d4c266048":0

AES-GCM
NIST Validation (AES-256,128,1024,0,104) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"3d58cd514de36ca7848aad1bf4d314b3b3415cae1ce9a16902
1ae84a67d4ab69":"e1c2e79e3f64c5c64f853ac9ba1a853fbf1bfd3001d48f7e73e0e97aa1b8ed1f1a7066178e75df688c
5edb1c42e270ea38ab0e246c6a47fde4c3141436fe4b34beb9033ba7eebfc53cf1f6c8ae1794e9bb536152d196e1b9680
3316a05f1dcb9016c8b35bf4da06cd18da6243acc3a3dc641d3a1332b1915932ca89937cb0327":"4a1c2e7a3f9788c3c
2fdd0dcc0cfe84b":"":"50d63c660a2b4f8e87276c5f58556cdf15d0fbb2c8ea5e3266d28c515643109aa7fc950d6d48f5
04dad52457e16576b581d37574574cd8b7ac12b7d59b819992c941a27e23ef9f257ed0c4ea4eda6c1f3b28b44decb63a
92fae84c3556dcb9d6458e729dad6a7db9f7411690fce971b3b240f8f9979ed992f87d76e227fd7384":104:"ac842579b
dd1ac77c84dffac2d":0

AES-GCM
NIST Validation (AES-256,128,1024,0,104) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"b7e4cd80f03a7ed092c776b243dfad7776d9caf3e679939038
e33ac94d8931de":"102e2d2c0d01dbc69733d2451d1ac1817d60418685d4ae8aa44e1ede1c1e08d2f71f0aef41a72bd9f
052ea4a9a057330c95d964f8c3679b80fc9c0952b46f38e2ef055cb33703d686757400210fa5a39bc7e3bb9b8b9cc20c9
5d5607e2f10bb5501507680ef3aaad96553333b1d27bf2f7ac102c983eede2262a5c6237c1d754":"af160a983d674b7d
19294f89c3c9307d":"":"6bdfae299d796ef36850327b091ba7bb02e29b643ca4c8bc199eb91ecbaf88426412cfd5570e
0042cab735cc46ec648b0877955b3f9a5707d56c478aa77ae5510749beb1e44dbbb37791f18477123436a985e5e9f79f
da0a057504847e4ecae841f24e1b53076d3efc6bdea2ebb336ee0e4b5e6ea973e3e50a27b5c2e6fee3e2":104:"fdf21e2a
c356e507745a07fc96":0

AES-GCM NIST Validation (AES-256,128,1024,0,104) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"3a0c46eacfe85cbc0c5f527b87cd075bdeb386d0ca6de816a8
7cfddcb8a87ae8":"6d1203dc8395e35a35e234203625ea9d37d1c009db2ac8b1d5b29021997b5421f1d172f4c9a7eb7d
bb67f0002720fc412f5b1550c739a2d7ba4387a1f978bd548fe6169d9473893782b10fab99198cb8b4553dfe27583c017

136fd8c95070d8d7f9a602d15248d38d728157a0b26404e662f9a5554d3e1582bc0e12f0054792f":"b1cde63ad2ad4b8a7bfb36ab78385c3d":"":"9de3a45c976d32ed2af5074ef13b1f86f35b1689b1c698b2e427d5dd62556eb14439f77cd8fcbe686a9a08a922e3f54a78e86fd284de493a740586360b63da09bc1d001777582969c679db54a0ddb8d7dfdb46750edc882804a1c00e417912b72b4cad54dffa1897eba6188b3e61ebf0c3dfab292c2686dcb9db3012e0788c7f":104:"641896daab917ea3c82524c194":0

AES-GCM
NIST Validation (AES-256,128,1024,0,96) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"4d540e0ba27103667eb4511ce9d243592bccb8515ab59896c9922cb5f1b47a02":"d79f9b1c74e3141f188704c8d5bdaaf6083642be50d00f20c97b56646863895250d131e00db0ecf4f035d42f08cfe20f401c2d3062a38daa0b9e7c19fa7c5d344680aff48d506daa181451f6b34ed9099b9a5b39c0166e93ac4463c9ad51f48e3063b1c16793615336f55d516d079f6c510c2891b97aaa95e5f621e3b5202620":"a2ed37daa797522a39b01dd206d06514":"":"6a891bd289ec05990424a2775287f4725aecefe1ab21fa0ca643f37829cae9fcbbf805b883f807102ff12f1a85964df818057daedd41c7349ef32b24642186c45d2858c3260d5b90594969e26b691963ac7fbd2eb4eef466ae690ca274d9194dfc4df1c3baec02abc38fbfc0e2c7c4fcafed227d4f6607329f57ee439435c714":96:"9074ecf66bbd582318495158":0

AES-GCM
NIST Validation (AES-256,128,1024,0,96) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"151d7e4db9e21c87bef65c2ac6aab5b6b045b7dadaf6424644a91e04ba810585":"0984c5d3f68beba1db4e6ade429cb8954cccaba9fcf4d852897ef69f8483428932c8f18a891f54b68f7d49a03c57f7144d802eb996d233cec930d5eb19f43d0faf9c94a2d7aaca40c8066a2882481f521bb5f6ba15b213810da373817eab3d52b5dd143a1521239482fbf4a07fe68c3d35c90c6ce27b55e40abcf432a261dc58":"49e0e0d089e3574fa5a33c963b403ccd":"":"6938d8a7625d1291f249ef1e086bb030ccdc844a9271fee16db60e7acfe4aedd720de76345109d5e6849fd1576c0fe0c34e73dca4011f8565cffccef427198c927f19f63b821f43844d008ceee0566f0d8062d7860e92ebdf21dcde80039a04504cd8ee94874b2eeb038962a74ac9902d9d7ce09afdac7aa706bf3892de19531":96:"48d3a8116213f92bfbe86bfe":0

AES-GCM
NIST Validation (AES-256,128,1024,0,96) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"3e9615515ca45109316cc02bbf3a23406eeeab2092dc6614db76e4e047a3b023":"46c4c6bad0f21172094ae07a47fd76477b69ca75cc08970e8dbf7b8644d4bcdce96f9d15dd3fba5fba3f851af145652ad004ee525d180d2f3e03bc0ec1c0e8ffebc1474c342732b7247f657ba87ffcef9333857123f29c4976b048c89c24107529dc5dd69004fd176eb0ca6ddae1df7be7d28b3b9da976413588f20c1fff488a":"c1facf73da64e16e4acee3fdc3cc6b10":"":"4415dc96d3daf703d392ba1318254143a58870e691570ca6b1be6074dd9c1feae12c72f9314fc3d19b6affb59b642ade6c4e64b7c99f850bff781de193cc0a321a29356addcb0918a282e53801541b5b01383fa7624c36d1f67423f02d2b54f58deca582b7031d192a4d32bc154ae1149cb3c5b48538c803a8d01fa7cfc1683f":96:"322d8d1b475a7fd3d0c45609":0

AES-GCM
NIST Validation (AES-256,128,1024,0,64) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"52c1a14b4ed57cbfa317fe0db87528f4c5551deb9ffc88932589e3255b1d3477":"eb9081e19b63c94b5f3a696c5fc2c0b7f434e1574394d0b41dd67dfac28a73d4ba26c86b3728b2802fb9d0930c89586b09602900d33eddc5a00a4e98881b5acd5597aae9b80b1569ede74042948f2cd66c3eeae227ae10241

df001c85dfe8a5fda0aa21142ecade76290dfdd4a27b6ff3a932dacc0b5f461501239ae8d6d5f41":"36d02604b5b24f49b08bb01053a23425":"":"12fbea9e2830ba28551b681c3c0b04ac242dbbde318f79e1cb52dba6bdde58f28f75f2fb378b89f53cef2534a72870a1f526b41619c4b9f811333e8ee639be1250a5c7e47ecbee215b6927ecffaf7d714327b2c4e8b362b1a4f018ff96f67557ca25799adfac04dd980e8e33f993051f975f14e05be8b7342578d0c9d45b237a":64:"01e6af272386cf1a":0

AES-GCM NIST Validation (AES-256,128,1024,0,64) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"4d08a07b3e94025523a4a6415029c8f9e11fbbfd72564964c53b8f56f865af0d":"4ac7c27b07a4aebe5caf1de0538d13a56e8c11bc73713bf78c7abbad3b9f6d690e00487267da108e2f2ae67c24b4657e77bb83e2d5e4b244cf34e924cf7bdb443f87ac8cdb374147449f8d06eb517a25dc86f03a389f34190aed5a7faace03ebf646fec2b173b2c15fd5cbe7c5affb6c3ee6d1cace8b00dd8f668a2336da5bfc":"98b745c7f231ba3515eddf68f7dc80f4":"":"337693c5c746d8fcdf7cd44d8f76a4db899402b891176e85b4c549c366ad709322874e986d6b939a350d2a0e3b77924d6d15454d882d1d3c94469d749a20d8f0116504cb31888a1e81d3abf25dbb7a7f9e7def26b9151ee649c059da1955f1716423c734dcd26a548844abb6b64c44383ec698e59361b6582c6883b77c338342":64:"7a9266c4e5ae48f1":0

AES-GCM
NIST Validation (AES-256,128,1024,0,64) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"b9d9fc42b58deafe9bc9734f4129dcad34a2e55ee5ad8abcc3f7bc42dd2c0e05":"11dbcd6cd53d2af766a1b6e4af2bc8bac2811ef818da2d1f81c140ab6e0298e958fef033736bc6e0dccd660b9a3e4222bdf3f89a95b206785d22852201e6dd00b44232ef3c03393893813dccf1960410b50cf50602ead8bd246fad88e66c88b50821578004779b6c45c13d8211df1cfc0fb2d7a342f58e4f2f3623fd31b12c30":"67931493096f4550633c322622bc1376":"":"66ab6e7a547705d8ae8ac3cb9bc5fbbc18cd220f89aec7dfbf4f72e7bc59b483c50c9471523c3772efc5deee3a9c34c96b098842cc42f9b7d7c0d2530f45900eeb9502e4dd15363b0543c91765121fd82fcc9db88fe6a531b718c1fe94b96a27856d07707fced3021cca9cf4740833d47091797cc87f57f5388b48e2296ff352":64:"0de60d4126733404":0

AES-GCM
NIST Validation (AES-256,128,1024,0,32) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"97e736a63870546ec9c2325a8e367c8ea17a7ffa71f6cadd6909a5bb9eb12814":"608280a9dcbd6dd66100a9fdd00e6dac2183e32c945b2b4d255c048243bfea15aad1a10ff3eec0ba79c531239b489a5dc155dc2775519f8d3d2ed82fa7ac653fb7c77e0dfad1c175b6c69963f5c12ff9840f18e0202502e9d1e3b170965cd86ae411af20e6d69a608c99ca8dae3cb3bcce666841132a99429bcde490d9f0b6b5":"d35192b4d233507b70c6d32f8e224577":"":"568a0d584fc66c876b7beb9ef8709954a2c426fb8c1936b9024181ca2cd3a7684c412715c11eab80a181be0238e32a2b689e9db36a2ac87db651058080531e7b1110938dcb09615e385d7b224b11222469145f6fb5f4c0e87b08bb3006bc5b6d2ce0a15be7fc29b27c10c645afd9d8253c094fc0f775086bdf2adac265b474d7":32:"af18c065":0

AES-GCM
NIST Validation (AES-256,128,1024,0,32) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"6d05193cc0885f7b74057ead3a0738b74eb3118b1a7e74c5c941ce0011197122":"c58f51bad815a43a5705c311de4a846ea2a70cbdd2c30d709a2ae0ddf82b7c889dc599fb6e0328fad21555a99530be6deeeb5b1beb333322c2b747288e52fad008513f8040a4735cab3c8cf32c4e18bd57339c85cf5dd71e382067bee7e9ccaf68e767d77fb005a3b73a51acf942fc3b2c5c9eec6189d01a26c6ffb070165874":"5160b65bf7a2ccf77f

a2e3e0b3866f26":"":"64dc5834a63be414c3714f1b34feddbacd568c6466cbd06f665aa269187a160db79306a53b629f
edc1247bd892998fe3208b3105f6273676bbdbff6e254de332d02bc8842ef98d6b79994792eeb5be3a807452b14ae5b5
027db81421cc22936ccaa7ae1b77a145462634e424ccf2dfaf001ed4477b804e204120a1416b449b8c":32:"364ef0b5":
0

AES-GCM NIST Validation (AES-256,128,1024,0,32) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"6e8006983712ddfedfebf95e6cc3b0aadc23077055e500ae49f
ae7705787f2e3":"e3ba14c4e39ebad925997649872b8331f1700c8f98f80e58d92c85a84f2a427094d9d771b276a0d35
b17c0c030734399070a57345d4dcf082b96c7eb580618f7af8bdf036296e20379e74e29f905b52a0c46fe7d46201a075e
7de7e1a523a0492c1f228102fdb89f019bcd4571e041c5d37159dc487ec139fa37d33142fc8082":"e36e39d787394f140
1fc4b173e247db0":"":"4d5db4b65a1ca31f3d980cc30037b5d79d28280a31cc5d0274be77dad70dcd37f652f2ca999c9
aecf08fd2a02d382457a277002a1a286ab66f9e437adee00c3bab04f831dd52147005a989606171b6017d28970c89868
99fb58900e23d1bc6a9ac0bd4d8b5d6e3fcaebc9903923e68adae7d61cf929388e0e357c7223523d1ff":32:"d21637c0":
0

AES-GCM
NIST Validation (AES-256,128,1024,1024,128) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"cd8ec237009eab590dbd9b31e76513dfa3501701b1a706982
944441d996e1839":"9eef7c9a0fa3e9a7fcc4b2f9d210a97d6653ded7913f2fb2de825a0dfd78ae1cca68c040f2328009f
ffe62937d630ee9d6e0e67bc12c38c0b3d035697d4c2311371aacf41cce0d523016ee436a47d93af0df77011131856d07
2c718c310f0995b71530d70a3da881481f46f21dda62e3e4c898bb9f819b22f816b7c4e2fb6729":"a3cae7aa59edb5f91
ee21231002db8e2":"45fa52a0e8321d82caea95bd9506f7331923e2aa95e9238908f3ff30e17a96389dfea75e225e34e1
605354eaaf999a950f469c6e2e8722da5ad9daded6722baca00e5d1b8e63266ad1b42cae161b9c089f4ffdfbbaa2f1fb02
45d1a4c306d46e215e8c6c6ae37652a8f6016f92adb7695d40bde8c202ab9c2d70a96220b4b01b":"833d58f0bbd735c6
164ecaa295e95ad1143c564d24817d5f6dded5d2d9b2bed2dc05da4a8a16e20fdf90f839370832f9ddc94e4e564db3ae6
47068537669b168cc418ea7d0e55b2bb8fd861f9f893a3fdba6aace498bc6afe400fea6b2a8c58924c71ce5db98cfce835
161a5cf6187870aa32f522d406c52f91c30543ea6aa16":128:"c1df4ee60b10f79173032e9baaf04d3f":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,128) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"5f0b24f054f7455f5821fdc6e9ca728d680e8004fe59b131bb9
c7cddb0effa51":"d406138587fbcb498e8ec37f0f3d7f6b2faa02e6880424e74cdba67ae3468b6823d37fd917a7fede6b3
4a2f0fc47c520e4088766ba82a989f0d8051a3a80cc8b1e3e1e2b1c6620b90e99b27e65951aeb3936263fc2f76c1c8effa
742f53987f8a38c731a411fa53b9f6c81340e0d7ce395c4190b364d9188dc5923f3126546c3":"f52f7a2051047f45ec61
83b7c66e8b98":"756cf485b6a8e672d90d930a653c69fdbf260d3ea18cd3d0c02175d3966a88b70ab8235d998b745a0e
b6a5c92899f41e8c0b7aa4ec132c8cbb1bac97a45766a03923c9b93c2a055abd0127a83f81e6df603a375ca8cc1a2ee0a
8b7fd226226b0b19bd2e81f73c34dfafa4fcea08dd93dd4ab7e4b437408af91bff566068a5f34":"e58a03f664003d0ef5b
db28931afd16e7747cff62dcc85bf4eed6e573ea973cf615e4ebee40f35d44e18e391b391e98dca5669a5b0abbfa678348
36b122d1909b53acd50e053d5ca836894414bb865b1fb811d8af68b88b4a302fdedf27fdd27456e9aaf34a8d53c9c8587
e75843e09776392dbb0501ef41359c01e8980e5221":128:"258492b9f549d1b90555eafbe5292806":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,128) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"6f50efb3946f6a6dfe63f12780f764bb6ebcf2127d3804610e1

1f0bd9b68ce0f":"bfc89d5049a5b4015c9eb64fdaf9fe9f4be7229e67c713a7b368f0550b3a5e12ba3a4399c64f60b7157e1b289b154a494deadecff0d0686ab44fae2a34ae4cb120a7f00268ab551f41c16a05f8999157be1103464127a8a9bccf736c32db045124178c90472e664d8e67a2ade0efe9a3b048c453d2fb5292dd8d29e62d52c5b5":"63c1192ab7fc75c17e7812fd960f296e":"335cc5c8fb5920b09e0263133eb481fd97f8d9f29db8689fb63034bc40959a176ccdca6725e1f94f822e4d871138fc39776fbe062f07bf80e5c8891c2e1007efeb77c158ced8d6c002b04442ed35c40a2187a59c02339c05762942208e3be964736a431017f472dfd5fdaf8fb8c645cdb684f9632057b9eb755253b4b75e3688":"ca974942ae0f4955ca0736218e4e356145c1ef42135b1142b55ccb3fc5caeec630eb50e69b5a6f97c11d4b604189b27496623bb0365ae69f4150e201e72bad8e7b883185588d0a31c44273bae87194b1610114a83ec47ba68a02e29891de43204977fcd0d551778335fc77fcfdf3fd63e9e5e0c02930a0321ffb093c521cd0ed":128:"2f11a01cb0ef8dcefad9233bec44d6f0":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,120) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"ec566324ad9d4cd015821e2cd4ed4d3d507bdb3c65bd50acc85f690ef06740fa":"348d35768d7192415cbb92c5625f10edd79f24c56d4b821aaf80d7dc83e901ede6be94d1efe11a3acd16ac00aea8d0d4875c47522332fed11cdf0816b26978de431c89d2fe6d122b2d4980f1d53a97edc15e490a44e73cba9394ca4bbb871675c729c39de80d6678c71b1bd220e4647bfd20a7ddbefe2b7eec7276b87c92ba77":"95c8a544c4b94e9fbfd76e66f40bb975":"fa6f38f8e562a54bb2281dc9a7cbe0b981292fb00dc0053185550a300661852179d0f2beb4e7759b81316fbfead5c858e6fce73f3cd2c2462925dbb199a4e6c121d051b1b5ebf60e16d1e30f6973b19cf31830da30588fdfff6115a4a1f6d977a72583379a56055724581be5232b0d1b0ae88bab5d4a031b058bc8d03078dcd5":"8b4da79f3ae1ea35a80af2f52fc640055e6a3b92617ddfa79fe5d8a49f28ddf36a82a17ca0b3cdf1726700f7ffc09ae5b412d064fd52a90a76bacc74a0b89e38dc474e880a2b768ffa91fef34c47759a7b8fd7faa32a4fcb258349495e4438c7b2055a8f462729fa4e7223aa9b47087695e3aabf43afb32e272d536b257b748a":120:"b1faec277697add8f756391dd9c7f4":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,120) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"dd6aa4ff63efad53772e07e0fa7d6eda5e73be167620fd7c9f3997cf46cd25a9":"592b3a6f09841483770b767bed73498c286896d2ad3d8bd91f83f92f489b1e83b0456a54e067a79e1bf59eefc1d3bd35cecfba940811d06a06e9b8f774bfeff557bd7e3f0864cb6bd3f867efbe3f040d2384ae8e1a0e20ed38caa668159d3e33c4669478d00963a1152305aa2037a5e06cac52d84021234a7f5d46ab060bd03a":"6386e03bcb6ac98140ee0706b54c8492":"0ccdaa4f54cfea1026a4d26338b1e6d50a70b00c46147fe906c95f0a2fb5d92456ca3aa28a257c079eceb852b819e46646997df87b873bc567f69a2fae471df03b0e5b94511189eaeedd238a991b326963c46d53080f420ec9fd1a74145a0b155cbcc0b5e47fa69450c7eb447080e34868d640f923923b91a9e13a05c73550ca":"c1be540448f1e3f432a10b3cc1a913cc4046595f5a57bf57c9d856cdf381832e914088d3388199018ff26327e3001678ab363da9457ba2084f5aa81320f1a0343491e0b44424018765861c5db917ce14e91a77f7e805d7a97a17a288ee66567c5c01ee61dc46a9aa8b281438ed377b792e9539e311676f81c567339cf92b8e1e":120:"ce7e361713630ecaff81866c20fce6":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,120) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"ad3990cd57ce4e95342cdca4f07d7e35d575eb19f224a7c821b1f5a8c54d4bc3":"732809c29b5eeda974039b122b875aec2823e082ef637294658cc54f9bca88eb7eea87a366234f89919975d0e7dd2f8ea83198d5a6e349149a016a4b177ba43df2f3ca28e27b8566591d225ac25dfd9ea431cf1fb3ea530d65dac93aad47764a6aef8ec6903b6d145ea9a2663034d2a320690b92afd8032084b754be97604382":"fd4ed75d861da2cc14fd1054976c8566":"ab44689839fdf47e887b70fc1b0422dbbe5c1b50f4e704f9a435967ba8b70cf1e144a025d37292f628f9f7dd9d05557b65340090503201e8cf2cea2d6a73ea4850bd0931b90fd4a4306ba84b8aec99fed47ca1b16daee6c95c97e4ba0dd1fb130cd13f5ef77c5af96f61fa05305a3aca3775e927f72f08fc34bc994e69abaad8":"f48721b08101b35c

de1c4ce08a8ba0049185b9dd48b66ab9971fd67dee24f89b456e9ca19ac8a9b5b3b088cbd53898a8c2ac1129752fb7fc5
5a0c3e2e7266ff40f7a9d63ebc4ab65f47422fc17cbe07fcfda582fd1b8f50e840ae89837e84add8be17d4cac3d2be26bef
4aa8438daec9d2b139e442f99c32f2789378c8029ad9":120:"da6da2af0fc14b591a86359b552e20":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,112) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"30823396ac90db573b6587676564d09fa680906bd6eaa6b85
97e2e7549c9d848":"c55be5a0b8559e02de4667ba5656f7e46f5627af13fd34d327f6fbfc4f3a9273036fce2fb21232f8e
2ed115b39b0ecb9a119c8fc17070bbe4e34d3544d7117ffda5e1ef05e063b5a8fceb23158d7824d6a1eb4d90a1d0360c6
bd78fb24fdd4cfa35924beb4e090891d06f53fc52cdcaa6b8bba6772d549eb95b64ebf3756ae45":"496ac734afadcd54f1
a4372ceb5645fc":"2d582131f7071e80cde1b11106b7d79bb208743de759d40b897efdab018f4eff1f91d2fe67e27af25a
13f201bbe4446f20ac6b942ff7b32cf10ad1cea36945b67ac08b114fc616175a87437ee05f3a8b6566e9edfbc1beec0ed8
696b5d5c41a25ac43bf3ce2920dd262233ab3405d46f523894dcbfb6c90b6e911ceb93bb7fa6":"c9da3df66111dcbabf7
31c6891eb698ac3283780f526e81383e201244efe4eca7a1c84a3bfa9ba5616afb15c1f1af0f3af2e071df6c1d34a343c3e
3440f1a3e1b6620243d9e7d9a4dbda5981c3e876fd07f392d44bf3e0a4edbd884462ec2f71d36bde4a1b5792629da09a1
fb01bfdbd532fbac71887a05a7077fc119a4638d4":112:"cec973a27c42e31b779a6a91aa34":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,112) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"815f2b2f0b1621aa198eef2761380f10ac9872a5adbdf6286bd
f3386e56aae4e":"d16930c570414bb620e0eaa2e9b5d96e4424127e16461aaa5885c616a02ae974fb2890e73bade9ffa5
066eb88a46ac7fcf258d55733d315951b1b71c5e3c13d78d60344ce921966297a0f6361cfeab03b346a7fa4f83a7a0eaf3
7576fa33a496102446f9f31b06ed91b51672c879cb18d4e38fa86e156d5b1dbff27925922470":"0843984bbaa565ca24f
148e57a7d9c57":"1514b99c0ad3493c36fe1216d1a887a69ea0340101aebb03f60d7ed26893119e81e8b8c3f0bb4af5e
10a3bf4edcf257473be9dcebb44a9d912f04d97a556ecf020c0bed7ccef2bfd5580f1fc74b706fea45f8c63d8de6f8deccc
47a02dc86d3f0624e52f6f1dcd09de8000f2d98a4cc0896da6a564b92263673adf390ed909fa":"7506175acd64224b39f
890e498ee5013bb46fc571dc2b125ed5891b8ce8bcf42342f015fd2df5f4b9cc220aab52386bf2247d4163951e8646763
3f96c28bdda166d778855a7f60465dd2983232c9e53d5f89432407807b0402a10f155f80055c339451a106ac54438ae4
a945e60d5320eab0adad9a1e66d59b9d3cc53887811d":112:"28d9d780052b36dbe80a25d41d5b":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,112) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"d1325ecedb8fc0fe449de558fbc11ddebef660e47aabb84edfe
69837a6a9066c":"f9a4f7029feae5cf5bdb8385d6ad7d7da6a243c5026818e5a794c6cffb8dad3227964501c5a049b5a9
4a7ea2e24434e0868000941184444c5a971bbe575324fb6b51c5939f81e78bb11d85d324742b462ce8d13584b3882617
d0c94776f328a554f9d532b6515ade9fbbd2de1c12ab53671b7f7edaa7e20223f4c371c1f229568":"8aff702c40a8c974c
f24bf3c645169a5":"9ec2e851dee3834d4843aafa740f3aac4cfb1e4d3a7e3e77349113f5200768c3e9dc37481d6292eb
eebd2372db02ef8ac7180830c7187995c815d1d1520c3e2f8cf2a94993b18c828b53485073c8a845066772615b26d7a3
d7d3e7d81ad1725797153f7ba5e313bdec582c5482adf76b31c871cd42a313018f40d7e23f1a7f33":"3a93663aab93c6c
d236cba4db2c03942d9ebc669633936370c2834357e76f6555c34d40dfaab1e78a105da9092acdba8be89e2dbf72e895
18d55e09eb2fa1ea7da505484ad4531dba3eb853d1ae1a477355ea9448067b0adbc782d64ec342c7cb781d9dd8dc2b14
dc1c9ab5542b679782b8bb9b45ff6a4e36c513df169c8eddc":112:"7e682b0ddbe6c55091838616c352":0

AES-GCM

NIST Validation (AES-256,128,1024,1024,104)
#0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"4b92242268e598ddcf3a5a0de26d74356693c4dbca354e44be401f3d6804ea1e":"72dc75bc4c8f5bbbd9c639fbdb34afbb84706404c9e67eaee1959aa4b51eac0db4f975cb3ed8d8ca27f72f61c8562ec953a7b8745826121a7016e60e877dcdb046f236af3826c1ddf5b929c5bd9a92b0d5c23cf8983bf2459ced6595882b3dd0cd25da7eba981bba122623dae22dbdce05cf4e5d82d2cc54eb4f68e9e8eff02b":"3c292bbcc16c94b0a263f4d22f328915":"167dfab08aac8350574693b31210138f6b99cfb61ba7ade2e2abffe2255837a913c9afe332e8fc4b2463310df46492e7d982dcb70fdda2a8b03911e6be9a5c5621d0ae8ecd1cb390910b6702aad33394c25d1160b86687e25bb6cdc4811e3158bb85ba75548329dacc19287d9c004a0473029b77ca290fc47c1f96d9583bcd67":"c2dd42ab9bf3fda78032f73cbf7d28dd8e32c582a3b7ee79795551f133234d62ea6571a466b8e1af0b3d354b71a6582c9c8013d5f8a2c34eb3e848360adac1d5005cede58eae7784f32a31c40eec5a3f03cc1e7263d8515b36225b3515ebcf8dca2a77172c797d347ed3921ca0bc73e8ae56347134a6a2a06ae084f1ebb7b0fe":104:"02fb002d8e4a1d11bb0f0b64d7":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,104) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"c5c50059a61692a8f1ffae1c616158c67d276dcd4a029ce197ed48567e5ff889":"ab7e13923e66d0f600accd2462af74192c3de6c718a27052ef7c1302239c7fb2413df7c662657ca18228575ed138bc54f31663df548618e98d64402feab529d5bf6a678431c714df1fe24ea80017f455a8312bb5b710df8dd3571970404a806ec493dcb1f3f1ac980663f0b9c9823e0d0304ed90689f70d4a24da7d8504c5b0b":"920d82c6b97a7bea121f64f83b75dc65":"a9bd57db2bbe83177287e5f614dab977071abfe0b538067f7d0c5acd59bfba95dfb725b8e1af4573ff10ce135148a3bab044552348378d5ff0c4f8be1aef7ed60bb9a374a6c7b8097d7c1804fdf078f212e63e9f11d7404ad0d1a9cb28d5ba199aec3a6c41b9e523b541ad38cea763159836ede6371357ab1aeaedaaf4481c29":"8f7e87e3ff4f7ccd1cedc1df125199cfb588339119a5ea5f9bdb918f89ca35f9dc16c6465fb25ea250eaaa8e7f00aca2199f92a2c244642bd15cbc9b62caa58115ef01d0b4a9e02527e035744b20892f79b07aa47b6c6db1332f82434764c43124b27148f2f611766781df8e4cc0b5ba99b858c13c233646dcb2b8749a194f08":104:"65da88676d2ab3f9c6d590eb80":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,104) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"4c7cc3588436ad9e877de72578d30026d32746817ca7a8fb7df9870650aa48d8":"00c2845fc495b89f870bce714f8604a7e7a96ede92c4b9bdcf044c9a176f66a28761089c083d5e2d613c746711238477c0efdf475e18af99e88cf76d04d4e40495ea16c462801443cd7f69c5d36ac9f337e828c308f1d1938b1fac732274459827cf9806c1661a247167948a93eb6e998a4cea76bb825baa27e4180e52633bb3":"5e82285a3b332c693e427f9410564489":"9971b8e234fc3e1e9644545e383eb065e1866e2faa6513278d3972add5ec0e71b1558329fe1ee038a27919e43bfdac8cf08141ab540528f74f9d5bc8c400bb6ee7867e4dbc2aa081d9126ac374dc62b10004d0e233dc93376b93c0da415e7d3e09851f2084a99feeb25939e21893056870cefe7cdfaf49f728a91ea0eef605af":"ab7bac4ddede796576e1fc265c3c598055827be74dc7ed8ef172d00a648da56727767d68fcbe6c44e7272dc8cb15f03a26dc439178849b0e9ad6c7410dd4cca3f9ef40ec7c280042bbc199155c7341e88d35e5e8d0b42856e618c6c30e43d49506ccc3518585c951a3898409315e8b3b4d0adccdb561ddcf1b9d3b2cf3de9750":104:"2474c830c6ebe9c6dcb393a32d":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,96) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"9d73aec506e022c0692892f6dbc3b4d41e86b97fb377c1956ee27b9c9ab3b32a":"f02bf60f10ed876a803a96e75f3fe17b4e355246135a0cd5497baad2a40a523c27e27bf848f0cb5d0c6428d08bec9590b17fca5e697990d2a6f7d21080ab614f378a07461e7a6207229e0a087e285841ef2f119cac7d8a2d3a

bbb1e7272a0d7dd493c8c4f797e160c36e086227ceae4923658365b2d3a3fbea11aa2fab3499cb":"bbacc081a6107364
dcdac83abceddbfb":"77e1da090e4d3a892baf1afbc12a56201a4362d8f09cda5e9bdb23411e6908915301d66403acb35
24898c1c51d6970a71878accd0048cb6cfbd4bf941c174ee05eca2c4a29f1c24e936d3a63cb6cfa710617af1bbb41d755
b2f79e135db914a7dd00c590cf741078eb72c3ab559787213202dcc0a4734bdd612b917e372f0e61":"d78fa4024b8d07
3899ac09b8151c29b10a37793b76f04921bdc7dd3d2ef530a831e53cf6a7ddeec0e033ceeabb525bf5ef57bf9b3661ffb5
7d3bd4024252fa11dd569102c787c2d8489a1ad1290dca2e8edf82fbe6b5f83bcc0e888045b895e20c8556ee80430cc86
40fc070491d2bb81a1209428938cd8e7a27e0e858029421":96:"2235d00a47d57cfbd383b69d":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,96) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"73198dfd92d26283637e451af6e26ff56e3b7d355ed7ab8b20
59c1022e0ea904":"2471b3c4cc1d6884d333d1c998c7c441808ca884cb88173a225569e1689ef39e266e9ad381926ade
afc2daccbdd3c9457ea1bdc3bb05168ef1eead1504d1d44dde34f96e1a7f2a5d3fb33cf5292d52fa9412800419570db0eb
24fb74d55de202f5df74073c5a2eb9eb726393996eaeb32072bebb00593de41b97ecbab2554186":"e36403ce1acc63bf
50b47387250ef533":"cad023cfb73d08e5b082c3061f3a6502a1c1d53038cfb19074d0ec26c9b272db93094147ef0ab2
bdce440a2b3233bb0429add47601f011df679698264c0f81444aba14576a1a565e5c169f967c7571bfb32a2a4d7fcae89
7863d78964c5b1a040cc845494c0ad8ff4353317b28ca3798e6252d5015b58e99354ce6dfbe8b7a95":"32afd6d6fdab2
019ce40771b5298aaadf753d1c4cb221f01e4dfc8b1968f898188fa4d448d8364510a7e68c7393168efb4b4ead1db1c25
4c5cea568a84a997a76dbc925a6c19a9092002629f1d9c52737005232e5c7620b95ed64741598a65a9ec95f2c97b6b78
bd85380811c11386074b1e1e63b9a7e99d1cb2807bfaa17f0e":96:"e22deb1276a73e05feb1c6a0":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,96) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"1dcbd278480434135fb838ffcdc8e7716e95ea99a1cc36d544
096dff9e9aeba0":"da3b8c9e4aa8443535b321c3e9bde3c6742cd9f228c971257430b27293ebeb635917d6cba976c819
34c3077902911169e8c6197b2d56a046b7ff03b482c38172accac98aacc90076370df28bc8a2044c393c7541b7b69b0f
b852746dcf3140ace4e76861975814d2b5966f7714fb6cfe3e4299d79182fc63a345067a0aa54d8b":"b737bcdee4ef83a
a83f124cf7208a671":"49a544aae76b04e62211428a2cc3719e4451f3dbf9a23b6ac824fc472e95e38386d267415c1472
a8b0707b0573b9eb2a39a5d5a13464947cc3a7a7dd3b7196f11e87ab5233944f7cea3f4d62b088febf8b82a44d4ca6148
be1ba24905432b7ac2bb4ebaf22d3bce97ac2bd34158b6011fbac77ee1fa96ca0c9c9e0207044fbbd":"061b491b73f925
0798a0fb1fdcd72a70eddc9cb48c1f10119387d45c50d5fbb8b85592a7977487e45342fddeb8d481eef3b99463972f66a
cb38fe04953c223c5f3e02611c8f33cb9ad7466860895fae585d40bc78ec14d1cf17b4c5b75e4d8c6341f1eaf80da4a78a
aaa30d3bc8bff15f234aacbee4067a947e42275b12e0bdb":96:"b897da3061c77aab5eb54622":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,64) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"2e00467f18536ea6b4d582b2480ebee883e4f56bd91af3ad7a
47ceea3ece9acc":"d5334398318ade59e6bda5cfce8e11b25c9ccefa2f651eb16f66c03d84dcc900dc7c85e6d2b778b155
ae4591af0698df7f3b8b9f64d4442ecc82035f7d8e71a5f61c515a963f2fba077f3cb8276e91b31b3f8aa193988a16a86cc
aec4a688ad68b5146925ec21d55ded407709d34d140f37e1f87d955619453c3704e83918088":"aa6716e6b7107876a3
321d807a810e11":"5606a0b77cc9020955c7efda33b7080e9c0e9fd374c4201b4324b3e6523b0407171141e8246d012
92a34dc69331f7177d6b7238e16e0303e85741f9cea5698e42fc79217d9e141474068d6c192713c04b1ba3573e93480f
69e4cbf72090d46d62d5b52e4a7613af8fcf0010d0024ea11c19cb04571c6d7045a1157cf81df18d1":"249119ace4e292
ffdfebb433d5b57fa1518af3389eb832146c3adc2dc62fcc9121d7f6461a53ee107ce7edf362b365d8bc18e50cf9c328cb
7c7aa7b4e8bfa07c34dc81c38fe0982bbc3b543485ea4b0ce5a76c988cdfcd241911cd66f5a5f9e0c97332bb0f3926117c

0437470717c63957aeba1c55d96b1ff0f4d6045f908cd4":64:"70e986fced03ae67":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,64) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"a18240f6135e7b6eac071546ee58bb52394bc34ad4e91ee678b72e4514fddcf7":"02f288eea5588e7a011f4d91eca232af70f60ae3d9302cae5a8a58798c1b4e973e3b1d07695934ae871201682554ef6a5b94976c6a1aa73d354f1d65e3f025bb2a3f1e93009e822a87590dbfd1965904223049c5ac0da8596955199ff767b92df10d1f9c05c40bd8204846c719c5594000cabd87342f0447e4e466c3788723f8":"149da8186ca73941582532ede16edf3d":"4d46e1e87322ca84d5bb92d58670f644083db06bdffd99fab0055a62b64a30b5a5673a108f0b9f114d379d3fe63a1f63407881c5b5cb03142109c158af42a00eb24d3b1873edd2284a94a06b79d672bc8f13358f324af2622e9aa0da2b11e33567927e81aea24f3605168e602b532fa2cf9bde5f8cc0b51329e0930cf22e3752":"36cddac99e2673588ba783d3c085b9935626687a2dbac9ad10deb4867c577d6f80453266b2400afd773e4edeb743c32562e85f7f8f43dfd87b10a2dd79eddf6e580aeb4cea92ac21cf49ca97398cc23c02b0ca59257643fb2bc6462b9cf04658352d53c2ee50d87cc5ca2ecb722d950f0daecfa0b7c33aaa2c91dd8b093916cb":64:"73cbe40df3927e80":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,64) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"4b64bded6c658090a85b5d889679c6a00579498aa82be1e3a628a1cd001e52a6":"182cd59dc1934199d2d2a2712157438c347e286f66b5a2b8b5149aa41ff7ba82adc3751be379741124dfcf05c531416a64f25f0d28abb6f7bf98c80762f0fa363da679437621dcf61bce43ef4d63178779d1a3ebffb82044d427ef522cbd2643cf1f5617a0f23103cd2a164a59f182b151f47b303c4eb7387ee5cb97cabdf985":"99aa6f359534da409a18540d82fb3026":"f55fd6255d8a188ce9a4a2727699ce16c8bc5c6adba88d94106038b74deb79c9d43bfaa47375148d843a5ce248d70193c8017196941b2d9e2dfd4375a3390c19d2f833b0b265dab30f26adee07ab0aeeb930dc3a9fbcf719a707fac724deb28dee2a6788b17fa3505290c2797c6dbf930b41eca1f6d54d75b820e62ec7023e93":"5a1211218174e60690334856483a3066e2e8d996fe8ab86d0f8fef09aba9ef0acff9d3e1e5cc27efb5464bc23bea9c778fc74206ae3a16e5fdbf99694ab7096f23c4b395d7a7b8d6675e56b5505ff62f52bf183bcc4433298296e41662d6519d9c1f0a5fb3140376c8890547eae72afe75c338ba97fad9f0184dd311bbdaf3cc":64:"8dbdc0746074b486":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,32) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"cadef353122cec1fdbc236c0ab195fc4d732655cef444c00b6cba5c61e01c614":"a3d5e55fa3110a268cf1414a483adab6d58ec8762a6e6be81269c0369e8840333503bc3688c7be001cdb84d163fa1dfb05f3b01ffff31151f1af780c796822e3d564f785964a546bcc2a320d81a2bc61058652a8594ae9b9b0917400e08d4a99fa161376ac53cba54c92889fd3497e233aff4e12cd85d57375c7c89e92cdf5f5":"d765b5954e5b486885dc78ce6801516e":"ba0405745971eaec5d337fd22e0ad287551e7084f1c9c38231d675719e3980356e183a99a3c760ecf7a8ede5e0dac8d2bc13e135570ff6e91a854ea3b457263b0e77896fdf7bdf0b53c8276cfd1ea3e8e22450ff2665eacd24e5fb2be89373349fc9e2967763d43cbd7adc9a376b1b4ab956ddf8b1a56d9385fb7e861bc34df7":"9b99f984ae26f9cad5b3c8058757a0a5caef0fb86b8ecef0c1bca6b99bc72b0d5345a00ae75e37d4e651008bb733105d2172edaaf5bda4ad950a49de55a514e882a470dca7c7bbfddde40d38fef4e1f3864fd7e212bbc0383d0bc29ab2303c8935d49c35d7d73df2fba0daeb5f37f9ab0d541766da71b33da1018a3f287ba312":32:"c374cd77":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,32) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"0cfc42773fe2d16a59da52234af5015271332344448c214a2b

4a0bb53b07a0a0":"dfbf9eaa46c368b28ef50227db97f29b5d9ed599760bb83f5d52f92ef5522815d6952ebb0d9b4efe8
844216d37510746caf8c775d2c862bad8d67effe109a0cbcdd14ba8e31fa420a475e55ac6b02908346ad1b064d5b6b86
9503e08d057ae65e9dc2a2a26345917b18d1b715a2372e8e114a071eced0c29cc9966d7205ae010":"45afb3ba2db9287
f06cf48405764a955":"16d3ad553cc0fde3f32112bdb478450c65c854927b198914649a2820a9e3d01131b693765d40
bd2bb74a50eb4cd7bc8dd8dbac9c6a61acaf5e4cf81570814b30a6a11877a8f9c5df342f70008cbf0576bd27a50bfaf6e2
2a40bd77435da16b666a06d172aa981bdcae0d25b8ab002c6c1994a356d3c3b7e4dd7b99892b0784f6":"e29db2c4bcc
ef2dda828ce652791d424a86cd5790e6ece67bc029ba9520bd8f35a214a73d8b86564df0eccdb60eafee4170da2694eb5
63e5a854b25d7ba0a4c53465fdc15c6e267be2e54263f97aa3edbe2358f3d9b8d28997388a57aa427a239a7453439359
3196253de1c2946b7a437a00480ecb2eb08dbe55ca2b3641c36f":32:"39e01fa0":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,32) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"2a840df4be22c70786c873058d2a6e16dd9895cbfb55b9c9e9
8f958cfe62e65d":"313eddc53f3986927a261f498283b6dc4a39d26f98c7428127237d79a11c5e626e2e9cdb68f72aa31
68ab23dfa2f5e03bc65a68d781f23fb9e295909cd9f0f3e5648cf82f3f6b3b509b0a333cb7d9f2b6e444c351a318f8f200a
921ccb409def21b87bc55ec211a76a518350e6ee21d7379edd004b3bfd1ce9086b9c66d80ec1":"ebf155f7cf55e6aabdc
1171c95c45293":"8abb8843de1766cfb8d6474496acda2f7a14e78a5e4c787ac89e6bc06cfd42173c35b3a75ddff644f4
a58aa7502fedada38a7156457365b4c3c07bc12a8f9061331139b9a2b8d840829b876beb84f27d5a64093c270fe6c310
ca3afe987bbc5ec4dc06358d5bf77c7b4e4fe4078c6d3ec28e9a281318da88949c478094c0065b":"769869a55754eb5d
6d42e22a2b5271b38533fc0c79642e250347d34566eeca732e0565f80672054bd10cbd3067730dbc567039c730d8bc3
2a2bdaad09885651533a4f03174d4e6510547c1e1dd51be6070ab0ca0cceeaccf64a46d0ef87c0311bd09973f3b588a4d
fb39c85086ea5d67dc531c287b83c161dcb25e07b671343f":32:"c364c089":0

AES-GCM
NIST Validation (AES-256,128,0,0,128) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"461566cac74f9220df97c1ab2f8bb74189a634bc752f7f04526
923d30506949c":"":"546d821e437371061cf3207f3d866c15":"":"":128:"44193072791c435d6e8ea7756a0bd7bf":0

AES-GCM NIST Validation (AES-256,128,0,0,128) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"7736dbb38f1fe351a7fa101d91da62124c22ac02ee06b9413f
56691067572f73":"":"5f01779e5e4471cd95a591f08445eb5b":"":"":128:"1a1f08c8f40b93e7b5a63008dff54777":0

AES-GCM NIST Validation (AES-256,128,0,0,128) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"eedcae924105c86190032650e2d66cf6927dd314de96a339db
48e2081d19ad4a":"":"a39d400ee763a22d2a97c1983a8a06a6":"":"":128:"3b4294d34352743c4b48c40794047bea":0

AES-GCM
NIST Validation (AES-256,128,0,0,120) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"714df4b69dc00067c4ab550f37ff72358b0a905dea2c01f00be
28cec130313c2":"":"c46d63d6fead2cee03bd033fbc2e6478":"":"":120:"2a0271b0666889d2d0b34e82bf17d8":0

AES-GCM NIST Validation (AES-256,128,0,0,120) #1
depends_on:MBEDTLS_AES_C

gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"454021ece9a87a9543a1626820d39edd1eff3dca38a287d8fb68bd315a7a2677":"":"51de54b633a7c9f3b7b2c1e4b47d26a4":"":"":120:"114708102a434e3a30088b5944c272":0

AES-GCM NIST Validation (AES-256,128,0,0,120) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"d7e90b539c99e8c2187ed72823258c1149890a69a9c0081ff8c66e1cdea9f2f6":"":"6dba3273560f30f118a2e0251f7b7d76":"":"":120:"5f45e00181cd2d7feb4723e0cdca24":0

AES-GCM NIST Validation (AES-256,128,0,0,112) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"2948233eec9bf8adf7250b20d62df9219d30e314c5932383203805ff9f3dc5cf":"":"d6b8e723272e26922b78756d66e03432":"":"":112:"14c9a9a217a33d4c0b8e627641fe":0

AES-GCM
NIST Validation (AES-256,128,0,0,112) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"c73fb5e732ebc1dc7c91ac25de0d01d427de12baf05ff251c04d3290d77c34d1":"":"c31220835b11d61920ae2c91e335907e":"":"":112:"9eb18097d3e6b6b7d5e161ae4e96":0

AES-GCM NIST Validation (AES-256,128,0,0,112) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"a46aff2121825814c603b258f71d47bd9c9d3db4c6fe0f900e0e99d36c8f8d66":"":"7cb5550a20d958490739be8a5c72440f":"":"":112:"8c76eebda0f1fd57f05a62c5f93d":0

AES-GCM NIST Validation (AES-256,128,0,0,104) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"61a612c76de551f794a146962d913f60fbd4431365b711217aaa4beaa115f726":"":"2d25462c90ad9a21073729e5efc99957":"":"":104:"e4d3b277dc9a107c0392ca1e5b":0

AES-GCM NIST Validation
(AES-256,128,0,0,104) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"4b233480239fabd2035a7c9207a8e1ab2da45a90a472b30848fe4b4757c628db":"":"50d45096afd0571e171e1ab1ffb3720f":"":"":104:"5393bc06b8c5ecef1264fd6084":0

AES-GCM NIST Validation (AES-256,128,0,0,104) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"dc051ac63e6b051594158399291ed101a3efbb1701b98819c4835a4863734371":"":"1f304d4d7f84ab560366215649b0a064":"":"":104:"1081dda9e0a793916dc82f7848":0

AES-GCM NIST Validation (AES-256,128,0,0,96) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"75f76df772af8e3019a4c1588a7d59925f80ce0d5647030f29548374e7bcc9e8":"":"d407264e09fbc853b131c8a9f808f1de":"":"":96:"d515522db52bb872a4d3f9d1":0

AES-GCM NIST Validation (AES-256,128,0,0,96) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"608d7592c094322b31d4583a430986bdf6aa639cc4b4a0b39

03e588b45c38d38":"":"6a631952e4990ae6bdd51052eb407168":"":"":96:"eb8851cfdd4fc841173c4985":0

AES-GCM
NIST Validation (AES-256,128,0,0,96) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"86a90631e5341e67dfa55e68b07522507b437fbab7f3e2e26c
fc6e89ef9d2410":"":"67763ee1890e4bb430ac3c0dbc2af997":"":"":96:"c6d11901b53cf6b13ac03cc5":0

AES-GCM NIST Validation (AES-256,128,0,0,64) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"b8d12783ba2548b499ea56e77491d2794057e05fd7af7da597
241d91d832b33a":"":"0365436099fe57b4c027c7e58182e0b9":"":"":64:"41fc42d8c9999d8c":0

AES-GCM NIST Validation (AES-256,128,0,0,64) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"eb17c1bbcd356070ca58fc3899bb3751eea5b9f3663c8e51d3
2c1fc3060b7ac2":"":"aca76b23575d4ec1a52a3d7214a4da2f":"":"":64:"fbcfd13a2126b2af":0

AES-GCM NIST Validation (AES-256,128,0,0,64) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"916aea7c3283aadb60908ec747bcf82364c1827ec29bedcbad
acbb9b935221c1":"":"e4aefe6f81872729ff5a3acf164922aa":"":"":64:"2035a7ce818b1eb4":0

AES-GCM
NIST Validation (AES-256,128,0,0,32) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"47b4b7feb91582a2f6121d12fd465967352e58d9f3d1bf2747
8da39514510055":"":"137bc31639a8a5d6b3c410151078c662":"":"":32:"822955ba":0

AES-GCM NIST Validation (AES-256,128,0,0,32) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"8955cddce65978bd64ef5228308317a1ba6a9fbb5a80cf5905
f3aed03058b797":"":"1370e72b56d97b9b9531ec02e2a5a937":"":"":32:"b2f779e8":0

AES-GCM NIST Validation (AES-256,128,0,0,32) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"7795d631f7e988bf53020d2b4607c04d1fab338a58b09484fe
6659c500fd846b":"":"f3f5cc7c1ec0b7b113442269e478ed81":"":"":32:"e4e6dfcc":0

AES-GCM NIST Validation (AES-256,128,0,1024,128) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"f9aab5d2ea01b9dc35c728ae24e07c54e6d1452e49d9644776
f65878199bc5e4":"":"96ec2252e51ebfb731b680729be73297":"983a102a67359f4eecac465b0d65908a487c98c593be
89494a39b721728edc991726e1fba49607eed1f8ba75ae9ab82a1a95b65ebdf48d7ee3c4a2b56832f21a483d48c8400de
a71537f4c459d1cfcf9d2cc97b32eb7c5146cbf44d7e5ac779e9be0ae758eafff2138d4c5370b8cb62d70ebb713dfd2fd7
772fa250590609844":"":128:"766b6dcf491a5836ef90f47ac6ab91ec":0

AES-GCM

NIST Validation (AES-256,128,0,1024,128) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"d713b33af57762f933d6abfecbac7fb0dc1e545dd7c01638b0e1510af719769a":"":"5da52833b6fc73c0e4b1403e1c3c10a2":"374dd4ebdfe74450abe26d9e53556092abe36f47bbb574e8184b4e0f64d16d99eaf0666fa3d9b0723c868cf6f77e641c47ac60f0ee13dd0c1046ef202e652b652f4b5de611989223b0acf1ead9b3537bba17ccf865a4a0fda1a20b00e3c828b9726bbd0b0e92fa8ed970eed50c885e6d69604278375af7b9ae47fbce4fed7d03":"":128:"6151956162348eb397e2b1077b61ee25":0

AES-GCM NIST Validation (AES-256,128,0,1024,128) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"77a1e4ddfbe77a0ca3513fc654e7c41609cb974a306234add2fc77770a4a9e16":"":"30d6ec88433a6bdd7786dc4d3693bde8":"69beef4dbdcdf4e8eeb9bf8ae6caff8433949afc2ffef777e2b71a99fde974797dfed2254b959430ecc48db72cee16c7ef41fa4165ce4a0636ad4e40875d193a3c6c56a6bca5a55bce3a057a2d3ac223eba76e30e7415f00e6a7643fda9a1bf4d4b96ce597ffe30c3f780dd767cb5681bb7a3fd11668380e272bdd70e66f18b6":"":128:"d4a3c91e02a94fd183cb0c9de241c7d1":0

AES-GCM
NIST Validation (AES-256,128,0,1024,120) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"303930b8ba50f65a50c33eccd879990d5d87b569e46f1a59db54371fcbda7fd6":"":"2b2b28d8a5c94b6f7ee50e130268a078":"c2ff20441d96bae4d2d760dcbae636ca7e01d263c28db5faed201bdb39bcacc82ebdc943968aa0accd920d258709c270df65d46d3f09910d2ea701c018ec9a68af7fb3d76a9b360de266b2ac05e95c538417fec59cec1f07d47c03511751978baebd2e0e4f7483f7351b5e61c2a60138c97b751f6a8c8323970f6be05357aeb2":"":120:"b597491dfe599eaa414b71c54063ed":0

AES-GCM NIST Validation (AES-256,128,0,1024,120) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"1e3b94f5883239c45ed4df6930c453c9ffd70b1c6cee845bbcfe6f29a762713b":"":"61155f27c629dcb6cf49b192b0b505d6":"5b7482e9b638cb23dba327cc08309bdb40d38100a407c36091457971bad3ab263efa8f36d8d04fdc4dea38369efe7ae5e8b9c190dad2688bda857e48dfd400748a359cfe1b2a3f3d5be7ae0f64a3f44738a7c7cf840a2e6b90ec43f8c9322c60dd91e4f27fa12197fab7ed092990879e964ce014f6be2a1ef70bfefe880a75d5":"":120:"7003f04d6b6d9dc794be27b9c5d5e5":0

AES-GCM
NIST Validation (AES-256,128,0,1024,120) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"9080effb27994ef831689da10600e7a219db93d690647457702c217b08057eb3":"":"f45514696ff5ee1e6e5797f7bcff05c0":"5251f800f7c7106c008c0122971f0070d6325b7343a82fc35f3853d25c878215e7a929bf63cc8996f0ffb817174a351b71d691f23021f58777f962fd1d45ff849e4612e3304ae3303ace7b8ca1a43f54e662071c183a1695873f5567397587283433d1e76cec1103ee76f8e0472814424b8981caea1f624131fb7353afcd2cd2":"":120:"cfb6d9bccf0378fabae08fd230edc1":0

AES-GCM NIST Validation (AES-256,128,0,1024,112) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"8c291f0ad78908377039f59591d0e305bdc915a3e5bfb0b4364e1af9946339c0":"":"a9830d5663418add5f3c0b1140967b06":"e43c04e1f7304c1d83235120e24429af8dc29dc94399474d06047fd09d61ddc682684776c81ef08d97f06db6e4cfb02daea728ec6ac637e1ecfdb5d48f0440d8d8ffee43146f58a396e5151701b0d61d5f713b2816d3f56d6ee19f038ccc36493d9ad1809a49aa5798e181679d82cba22b0b4e064f56af

5ec05c012b132bda87":"":112:"275480889efe55c4b9a08cef720b":0

AES-GCM
NIST Validation (AES-256,128,0,1024,112) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"96c77c11a3336a41b61ffdc1724a80735bbe91dd4c741fdbcc
36e21c53335852":"":"655502d70119326405d8cc0a2c7a572c":"c01034fc6b7708128fbf4d6ffa4b4b280a1493b9e1dd
07079f509479b365f55ae9290689f1c4bdfa439344e3abb17f3fd3d5e2f8b317517747714a82f0a9ace04938591d3ade6
d6095491a440322d347e8634008cc4fd8add7c1c4764afdb2b098b3f5604e449e8049a46b6192647d19cf88fa5ed1abab
7f313b4285560cba44":"":112:"b4d581464c4bb23433699c418ddc":0

AES-GCM NIST Validation (AES-256,128,0,1024,112)
#2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"e2a3957393669278f052ff2df4e658e17f2fe32811e32b3f62a
31a3938930764":"":"a6f5a1f1f1ac77a1cb010d2dd4325cbe":"ce9c268429ca9c35c958ca3e81935ec60166aea0be159
75baf69103251efafd54cbcc0bed76a8b44a5b947199cd3c2dee6878dd14a5a491a4a3d45788405d0129354e59c047b5
367f1158bcf4e066a276951d2586bafc3c11f8a982ca7c3ba4677a938498bd51171552ea032fe1bd85cfeaeb87e87168f7
a28e979b08358f841":"":112:"cd5986df8e9761d52cb578e96b1b":0

AES-GCM NIST Validation (AES-256,128,0,1024,104) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"2b17652f7f04073afe9d9eb8b2615c7550968b9776b139fcc4
f9b0300912cbdb":"":"9a8ac23ea74b292b7386138666a0fb60":"2732107241e6136f1dd28d233373079d75d6ac13828
ae7afc751b6f9c57e77268c52ae91f4ab3016af2764597994573cd6b41f72e21b60ffbb3aafc9487ac19d0ffe8db2ae2c75
05ae5963b032d1ee1bffb4c5bd88bb0c9a350ba26ee3eb8dc0a157955333e4f28c5ec7349c39229dff9f440da72909f287
0aea873a76545ee8":"":104:"f7b94229439088142619a1a6bc":0

AES-GCM
NIST Validation (AES-256,128,0,1024,104) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"16fe502e20d6473ed9a27569b63a768ecd428738904cf0b337
df510775804619":"":"431a8d78b91414737e7c6188328a6d37":"934bcacbac10ea4ff6ee94b17bd7379b88489fbf123b
f496c78c9b6b02ee97dd62eedd05b8f44f4912764920129e711701628991a0009ebc7017a1a19b177ec9bc3b0f280eeef
adfa310708dfe214428a184147b4523e66f2d62630d4a12fd3e366d27c3b7d1566553c9b434ed193db083160da1f241d
e190bcbd36f435e30f4":"":104:"1dd3e6d610f359cc4e98d36244":0

AES-GCM NIST Validation (AES-256,128,0,1024,104) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"ccc545fd330cf17e27d75582db28807ec972b897f812d6ed47
26d2a18daac76a":"":"caf2f56584a59c42a51fdbfe4ad78f3c":"e85ae6b27778893f36f130694af0b40f62a05aa386b30f
c415e292761cab36fdc39bf5687a513e25ed149414f059e706d8a719b7165044fcbd48c773eae546380b8e667b56824e
23685173ad9015a9449bc1cd0b767981efe09da43a07bf1aeee08ba05d387b8a00199e18c874fb3a91f77ba448c3bff97
1593f94747fce9cbd":"":104:"5cf5c7ca6fbfee63854f3bcd15":0

AES-GCM
NIST Validation (AES-256,128,0,1024,96) #0
depends_on:MBEDTLS_AES_C

gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"8340d604770c778ee83d0fdd5703b1fb304c3bffeb6f4c65e2d
d0e12c19bddcc":"":"c0a580465b1b2e8344f795a6578a5151":"799f228962ef87865dfcfa0addde7366de2e4aa78029d
bc8d57d7e50fa7c74343458df3465103556a3bfc5ce217fbbb5b2835c9f76b70240b40fd605bcfa6b790d5985a8ba5435
4e0625263c628e8746c451504fc58a179f90f77f2b293d8dbf5582b031082025c806e60143da9ebb6133ac8367376d05
72b32569ee799540ae":"":96:"318f56bd0f3832d043ef700a":0

AES-GCM NIST Validation (AES-256,128,0,1024,96) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"74de45262fe09e12c9ee7100030352112a6532d1874cc6792
b4da6950677eb2a":"":"9f7fc7367f9afdb67fd1afffac058e2a":"289ac6f5beecbbcbde5cb3b0fdf4a27ba237fca33719f7
74ed33a5fd35d7e49f76d3e88c53fd35561655c35469f3eefb5b2f776ff2799aab346522d3f003154e53f4ef075f016aaa5
00c76870e6659a5f9af197c9a8f5b9e0416ed894e868463cc4386a7442bb0c089a9ab84981313c01fec4fc0ba35829b3c
f49c6447f56a4b":"":96:"bc1b8b94ff478d9e197551cd":0

AES-GCM
NIST Validation (AES-256,128,0,1024,96) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"441ec8afce630805d0ce98b200e59f5656a5ce19e5ef58241e6
ef16cac7646b9":"":"a1cbeffaf55708c375dcfeb496b21f4e":"5a6ba5d3f5a7a4b317c6c716564c648f0e6bc6b0f9a4c27
affca6d5af04b7b13d989b7a2cb42ce8eedd710be70c04c0e40977ca1c2f536aa70677038e737064fb0e23d3dd48bc00e
bdd7f988f57141e164e3c18db81e9565a62e28c73770666ff3bfd725eebd98946fed02f31d500b0b7ab4dafeb14e8cc857
31a87f50d95fae":"":96:"aa4bb3d555dabaaeb4d81fcd":0

AES-GCM NIST Validation (AES-256,128,0,1024,64) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"d643111c973ffb7f56bfbf394eedac54be2c556963b181cf661
ba144f7893a62":"":"4575b00b9af2195a0cc75855d396e4e8":"b2c53efe59c84c651979bcc1bc76b0bbf5e52b5c31158
49abdbc469a063e2b1699bd292e5fcb3476e849c9edbe6ea14c2ab948ed7d21a21f69406621d3d412b043eaf813be722
d92739a33a361ed8081c0eb00400c3c7d4e329f5ba4f7b75d534500f42f178048cf2e95b768ffed79c350f2ff72cb355ab
db30af0a1363c0b4a":"":64:"9d1d182630d7aeee":0

AES-GCM
NIST Validation (AES-256,128,0,1024,64) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"91301ee0ca694ae6971ee705f53c7ec467f4c88257d6466f6f8
159a8970384b9":"":"345fb57e88124a414828730a85f57871":"c13623824a204385f352388098f5e2db23426f00a73c
60c1bf1047ce2c7cdf7f7cc8475781fe7075d1226ad18871e12f0156f35e6ce7032efe3bade1c807f9eedc720fff7a27a2f4
690f904be9c99b54a65509eab60e97c4283596eeefa2b2517e95de7620382e3f780efa1dbf5d3908373adfe784a4faf298
681e171bade4b3":"":64:"325d08c5b96068c1":0

AES-GCM NIST Validation (AES-256,128,0,1024,64) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"b6ba5c11daed7f868da9bfd7754d555a147a1ffd98c940c1cd5
d136680e05c10":"":"b0c92b79d78547496d770678e1ce1552":"5b1ac8ff687f6fd2429dc90a8913f5826d143a16a372c
ca787845cea86d9b4778708bc0aa538f98e1031850f7c1d97fb64fe29adce6e1d51ca7f5203fc0358fe0bc54347e777ddd
fe04e3d7a66a1d1e2bdb8b8929e2100daf073845db5dc0b243819754c4c08f4fc3631d1cbd79ac7604746d677ff035930
fcd6bd652e7864db":"":64:"b1819b6f2d788616":0

AES-GCM
NIST Validation (AES-256,128,0,1024,32) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"5fcae1759209e784dae5a8278b267c414a03ce7c803df1db78
15b2910d10ce19":"":"24c5c349b3effebfd076c88a591b8301":"ca2778e39fffce7fbe8f912e69d55931848dd5ab0d1bd
32e7b94af453251a47f5408ebacd7b50ddd1103fab1c72acc0a02f404c5661d8450746d781e2c0861b6974ade9ee2515d
a88b470f16d5f06007f35ce97cfc17fd015e438af39ca6127db240babe9c42ed5717715f14e72f0ef6ff4ce512de95a179e
60d6393e73f216a":"":32:"8e59f30b":0

AES-GCM NIST Validation (AES-256,128,0,1024,32) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"8d71a70fd58125b0da8dddf8d23ddbe0bc44743753bdf25944
8d58aae54775a6":"":"d15b02572dec98398ba9e68e1a463738":"81313be1eda9f27e01b30877ca90e825f55ef60b1554
8c45c786c44b024e7198f333be7ddd2c3f593a9b77b68e6a7ac4cfc015aeec66f4823d9be7152f02a533f375554309a4d
b0fea8e76255144458e488fd19106d9a9614e828ae306fe82af89e7981369b2259c49bae77f8ec2b1f169ef0449ad083d
11907234b72ed2e464":"":32:"99df1b8d":0

AES-GCM
NIST Validation (AES-256,128,0,1024,32) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"b52398c7c75e1b146cc9998eb203159925cf6fc0b1c993ba46
528e2f8e8087f0":"":"afc9a60ab8448b77fb05e8410d0a26e8":"770b3782f0e3a19d7d6bb98fa3eb0b916928a2970701
c0f4a372a0ecd63499444ae02fd269ddb7d92e11a9e11d0e0b8bc60096a4be79a1e063174b710c5d739d8d05ab5c8ba1
19ff40843cf8c5dc4e1bd6fcad8389de3b606284c902422108d85eb3589524776641b175946c9ade1465e0d1064c5ae0
73be90e3261878a9af98":"":32:"32d6b756":0

AES-GCM NIST Validation (AES-256,128,1024,0,128) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"6793869513ac886ed66e5897bcfa263877d8465fc762b1ed92
9ba3d08615fdd5":"cda45e29f487f21b820e1af2c8e6d34a8bdf3f72d564a4625a6e06f9bae1c2eac3bbd5c5958fd75cf3
89a1a31391211745029dcd4cb2575f40ab04710a909b88c2d430cdee279f54cf7c0ff6638d1e0e631f526ee198cfd6e5cd
f73d1a11b69de01d640f385fd829616cd2c0e78f09b5f64012e42dee9eb0245b72aba1404e0c":"a43de15dae25c606da1
e7a4152f0df71":"":"385834c853772af70675b6be2d5087df84f88b6a303ea594a170e6dd0398ae270fcec61661ca373f
4653d8dcc9e71767568c0fb03023b163bdc9ae8a08ea858cbb03b8182b4674147cb35ffda14a2f50ed9eb48d5351f00eb
2fa433fdfed6f94833bcf656a7e350eb978a0aaf7a91674145f28f64693197a116b21328e273dca":128:"159ffdb056159
41e11f0db46ac8f23de":0

AES-GCM
NIST Validation (AES-256,128,1024,0,128) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"9f77c141b234907b38fb45f1b3602f3c29de1ed839bb7ba51f
6192aa8baaa287":"96dcb74a78e99676a71673e3c9f94c34b34dad2748a6e42cc70ea50e41ef8b86b5992295d2cbc8d6
21fefce09e8948de7e696b9788377d598796afd002a82b628d9890db78359e1edc075cbc0d3f11d544bfdf5c8a838390c
b856735942dff260189c00accfabf720e5fef1d9b7131a6b2b769f67374602d1a7ed9b899b2c398":"1b4900578814866
5cef20d8dcde41889":"":"b4ca59caaa94749317789b92257f2ef1dd3d9b1f4ee9540927a6ae7bf5bb0b348fcf25ba8ddd
a79a89d3174ac1713421291910c8926cfbb4ec1e59be7dd50e816ff586f165c605371ee6077ba4ac0ce10499f9a2a4486
6ce6319fce22652226164cc0a813c3147c4461dd0410e3701d4647d5a003090082e367cb9249cf1be47":128:"8048ae0
c35a656fcaa2f4c1b6be250e2":0

AES-GCM
NIST Validation (AES-256,128,1024,0,128) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"2419fd9dbe58655122ac1022956a023446b7f4756163769fc1b99eaf8fba1474":"93bc33dc647c7321152b12303f38937bd191ab3ce3b3a43a29f6853b33e415667d97192fcab2d1baa017042b301d03bae2f657505cc58e3aa4bd849d1ce85ede0e192a373a3894c41c54edbae29a209e16c87c81445d43968595297b50b55659f8b92d7282a2b3ca85e4b5d4ac4ff5062635103f2c7806fcc7378d5c2013be72":"94ef13dbfe9f362da35209f6d62b38a4":"":"3db23c161cf352ba267dab6a55f611eb5fff78a75288779a167cd0e4db6e75d21f11f4ff2928abcb1b46d82c2a0b1f647c60da61f9a72565f629b06a7b3fe96e4141a6886436859f610724bbe43fb99fac9b78b1e0138e2d57ce5fcfac1599bdba5701cb424535fad9ac482ab381eadca074e7376101b4b436f9c43ed760a0a6":128:"ecd4a7370096dc781c3eb3f7e5985ef1":0

AES-GCM
NIST Validation (AES-256,128,1024,0,120) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"08e11a8b4b24e63060c5002713725bb5b4a412f1d76eac13989738ce94e19642":"d5598f4e37274f3b617aa4f9cf6b8547b4eb1e0eac79f6eedd6cd5364f8891f66b8d0cb09f54777d461bbf92d6fd74b3fac412b77f2c48e1024cf09b83c1e71bb86f0a20f82d296883ffee62a4a192b184bc6d7ba0448c1519310c83b18c00e71153137afad14f096b43d454f205ba6b6c2ec162aa992cebf50735dd9bb37c7c":"c6f1e6a39cabda1089048b536e39cf67":"":"1fdaf0156456b6b2a68d66091bf2260792748acf3e7bbb7906af8e0df3b569a7c03ee3a48bdfdff7ccd52433d0bbe8c5fe30d93633bb9d591dfad7d81bf8efd4d4a3c5c0bf2ac9832f0a8687f16be640fcf9b19169c251f46b97167d95115acdee3d4443df416275f5597a52c17a4b8c4b723d4b35a7fd0b380fdebd44df8bd5":120:"cb9f4d4610c67acfe612af5508bb8c":0

AES-GCM NIST Validation (AES-256,128,1024,0,120) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"da2dae0107c284ec2aaf6e7306959df1e92d3932b88954f119ab677c6b9dcdb5":"277675044caf1713109d4d3abf50c6fb67dc67f7fa584fb1a41c833feead03177cf4b42edac139807ede16eb1d9bed27db741f9542d437781405608de18418c9f7269ab3fd88f6a922a31eab5a3b8b2aa75ee4315fcea80c4954ea6613b1360b1c7c6b6da815e3f6e50f72b7e69c3b6cb3d154855e3f83cbd1947eb54018155a":"2005f79d55b12e6dfbab7fedecc50e2d":"":"c2aaab524d1738b5244af642bbd16b32ba954e69ae51acc804a6b0f89f6cb77ba2db2b0e109cda6036786f9cec5587b01e306ee8b3d588748c61ad7fce1266165729d0153ee189746b107ce15ced667279a484294725e120dc1803d2c751784436ab8ff1d5a537628ee35742d1917dc51f8cb46c2d6b983bdec502e99b85e5b5":120:"52b4d7f2cc44f0725ee903551f681d":0

AES-GCM
NIST Validation (AES-256,128,1024,0,120) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"637807b3e472e2287b09d5a3ee62f791a416419ba35e11c49b24dbadc209f0ba":"e91a0a7320329dabb0d0fd7f099a4d313724aeeebcffe6fcea5b00af27d258cf9774845d29aaf5dad634c6f087c3311b1c92775fda8df8820c91186da30dc79747be6ec6230f2c261063143f4fc89d94c7efc145e68bfdbd58fb14e856578ed57ee5b3cba2cc67dd6497f05d1570efa496b46f5bcbf82ff9c6a414f76fcf3f5c":"46909d8dba6c82b86c7a2aca3c9e71e0":"":"13b4ad9c51063a7f697f3fc68030144aee0aeef0b5a52c9d4920a7185b0452159cf13e64ca216ff16637d0946a75fb5da283fcd263dd7ef2c8f14cf75537742d1f0e48846fcdbf03bc343203f7c31cf61b36374033462a7b813f4dbe9386e57874591fde606fbc150d4916c339f1950b09b1911b1b9119c3ff4053e05910ffb2":120:"6a5c83f807401d1a9a3a2688289f61":0

AES-GCM
NIST Validation (AES-256,128,1024,0,112) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"33613dc6e029df0f3ab9ca66fa96cdeaa84c1261dd586723b1ce873545565f7a":"775862b39c2a509afd3470a56891fbb79bdb7dacfdb9ac72ba4730cb936d364e1aed3c92c01a018cfcd7953f751003934c15bdfdf2826e9947ea8e521f55fd2a04c75156e4910f38932c9732eb3e60423e849d34c55e3fd00b48d83028e3b4f35686016126ff16c942ec859d3c3aa2ee6d322a92dc9fa9b0247423416f5a4b47":"59484fbc27cdbd917bb55f815f9faab6":"":"069f80826dbee03e6a3437e7c6d16eb6022bd14827b8e45bd440d9b1a8ddae09999388ba0b1be0a6bafdb96f26dad523a3592fa610d5091f68380f4c1c3fa9ef7a0796ab183e8a82c2bf1f76300f98ce983eab7a93ddb18f1c10534fdb61ace83cae37e225930ab870a46285e733788e907255ca391945d409d2e53dd8a28390":112:"9f31f8f8459eb03dc3654caba5c2":0

AES-GCM
NIST Validation (AES-256,128,1024,0,112) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"75d8132f70ef3f2d8946d296c83014683eb2a4a58b555c0f48e4bfa5774d6672":"a5be88fd43dc761838f3a9c7d62923c38414fa61b3678313cbc8fa9c2e5effb6cad7d5be5f39a71a28ff327b68a69f7e6a6bcb90eccacaf3a8659aeb905dd3e38efe57f2bd0d19daacae238baa01a7051084da6598fc5a3783a18decefc8efc8d46c7b1887f87d6d70c909df49340bcc680832faac3dd23cab5bcd80553dd485":"5ff41f3e75c25cedda1b08a41b89c4b4":"":"959396b86913337f2b1fb19767b787c18f00661c5d601bc65e884e15ac8043081459e889453e906ee267cb5d04fbaf250144a56c820eca34469967c73daf50796184ecf74f3c054bfa63bdd0c32425a8e10546ac342bb8e38a186e42a403cb80110aefd5f2d0bcdd353daa4430b8e7ec2134925c454745e2f708cd0b90d9d672":112:"ca0889a0eb12995079cf9ba77019":0

AES-GCM NIST Validation (AES-256,128,1024,0,112) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"8d44344d2ff9a02b1c75785bc84f16e4d23614bf43b2b9a87798b418e905c532":"e5689cef9f8258a748a615070fcbf40ed0b24c077e2f9a362cb536737ffbc5383bcafed278d4c5e0f3c83fdd5cde79483c2c178f6fef05ab50f2b8db680027a175bc6d702d249efcd6cbc425b736f1905307c9303a4bd8aca620b57e3bb4b68f2a515259b06cf5365b675edff3457e2e915d7da1e0802f7300b3d56c4644f4ad":"256a983cd6d6eb4e80b5c1d1cd2a9f21":"":"13eeadbecc4c9991e2aa0b1ca819572ef28517528320db970739a16994f82cd8b5bb53d889f298f65c63dcc07089dbf7e9d00612d2cc8220b5630ca0262a698836d906256896eea446f6de4506e558b4f20950528c8c397b6b5b04890204b77a163e46c80c96b3e268fd2754e0380e7330782d606c771d6085b34200a80335f0":112:"b33ab1e4029998e2566583dd550d":0

AES-GCM
NIST Validation (AES-256,128,1024,0,104) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"3999a6a394943be3d6e5732af5faf26caf483a3fd42c13b7f4f02132e93a990d":"8907e8832553264d7e92afa1595842ac661ddfec3f4294567faa0af61b3d0fdf76a922a2f3affb36b3b3b97f18d5172aec0b8f6f01239bb750c0fdd5da1e1244473cdfade83797037ca46d83123e6105c5c54071971f190da0c59821b0bf87242502bd19d19c7f463145bab0e687a18ffb2216c4a2ad2caf9488801c33c78c03":"76e2a5141d094b3a77765ba328f33576":"":"995189a396486b451db0167cf6990557287074def46eef872e6cfe1a297e256bdff2b71668ff0184eedf00ff1a3ec91358874718f0af88acf2bdb191e97332dc544d940412363840d4c03c7b2231852393c62d625093011ef314e4f755b1d0ee37690b4dfb55194a1465714cc3cbcdf93af39e666be0407508b8764f7ee95d3c":104:"87c8f61f459fd4a09d9ee8b331":0

AES-GCM

NIST Validation (AES-256,128,1024,0,104) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"4359a62d54c43770c3a0d51da25cc32fd985d9b41c282887299d2e348aa25a36":"f020c9cafba399009bd920c3ffc165d4db47a9ee15ca8c1f51c65e306ccccd3f1d694071a3c765b5255eba6ef6a280f6095f8c195ebdfbee6968b57366e62e16d05b1768825ab7fe66300941270aa121b4fc02ab970ca6e32170cdbccb46fc548620fa1777049343b1600bfb1bdecec6682f0aa7244a0852adbc7aacedfba446":"5fefa85c958417b6bc8a61b5496fea93":"":"3b8f829aa1cc1532a434bfbbd25f42480311657215946b9216846704fd5da5e886ca9d130df466c3b58f5259102ea6b9ad756e9f484a38dd0ed289fea083ab99fefbc2747100071744f10e362351d4ffac6c7c1f5a49ef3c78e2dc667f6b3bfd0fec454c4e3139443da71e514540d7a228db193a4c35d639ec13c1198ee7f81e":104:"591db861b9060869edb228a324":0

AES-GCM
NIST Validation (AES-256,128,1024,0,104) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"0d798a357de5a686d06c329e451d7384bfbd462063fb8ea7d77a13dfa1f2aac2":"d920785bd7d7b1a2c9c20139380a6ac5f27a11b614ae110da14203146c2615d81e97649e95edb0eda71a0fa1589244ed42fd9449962a92942e38001ac64b212c7e06c113129712a01556577ae02325a26eb92581c0a690a894225e83ff1e36776f22b600508d6d96a0d1c55316b518df8d09769df5e8340cbeabaa0bf7752870":"50a003c0cb50ae8a3183cd640ea4c6f6":"":"9af6a5341cde4b7e1b88346ec481024b40ad95a51533cdd8e09e4809a20684f18eaf243e1df56f02ace9667264cc1c6af6b0914f154b332234f6468cc471ecb2078a9f81c17f4ade83d326b670795458d110e4c4b4cd7fe7f9f5f4d4fb23a038969e4ff4f74839b1edc270fc81fcdc8a0b15b9c2f0561567c471b783b4322ebf":104:"6c2f01264f9dbf29962122daff":0

AES-GCM
NIST Validation (AES-256,128,1024,0,96) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"29b01b6d15f6e68fc2e7079429dde5363888a6410191d603941bed272daef7ed":"123b6da306978f745d1dd86d7df32d9421523a7f329dd29ad98d2c309145844010295ef443a18d37ffe093080682fb96ba9c2c92105d35d77897b589e2abc7269aba8752c2a48c843bebad2c0fa281015ba85f5f709f6aee9b1d49236d5695f7f7d01554b193c89adcd1a91749138952cb3f0ec8b5f046328b3113aaa0715ef4":"cb4ac8373bcbf1b14cf2a6a6a16a422a":"":"caf71e09395d596d5a7b091c9e87ba6d522e974451e41f33f3e7ded554f24daa9da719e87793424eca9a3eb3972983354041091ba4b16c5c8c14913e1f6cbda09779188e9b5512917a0adf4b4344f119736ba6328897726a317989cddc66f16bab64707564bb0064fe6ab7b2b5cce143e94d4b6d739f58c47b6d4850697f8101":96:"f635ff3d8bfbfb49694e05ec":0

AES-GCM NIST Validation (AES-256,128,1024,0,96) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"f96d8cdcc21884e050f762c049930d78360b56cef5b99ae232c9a8c6e8fa89f7":"9cf05e5065531d2539d92ae76a43da1fa3614ffa4b1c73ddc2358f8d71345c01260060239edf629efc3650e0d13174af4294b6da0f39cc7fbecfa324afff89dd7d203416bd144c5e03df60a287fd4a8d54ef9b4b44b3d6de1d9de07418b8a34ec5c28cec3c5b2fb861583178a68ea0af89f2dfbfbd86f7cf1e572e1c8d4b0675":"5a7eb964b6bc9e75450b721b4d1f8f92":"":"566abaa23b8d464d6f107699453740e9e189254145c5132fe46989a6654de297398913daacb4083b29f7b31832079616e9a43c9c2878df1df451e49f1e629c8b9de2fb0e4ae9df48e3e8880f3f1ff5ace8842d2695e702dd1b7bfa7c25b0539b8c80d31ac91856796beced082c213e8be56efd646dae932f5bf503af46f491d8":96:"c049cce29c401d3d198773b6":0

AES-GCM

NIST Validation (AES-256,128,1024,0,96) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"253234c3dc9cb3d50a80598c5cde0e37b6b13bf834f3595a9458dee698a6d19b":"686ad2740bdad507ebe97aa5bdbef25b8b030c4cdcaccb0d3b675ca91279db3ea75aa222c0ae98f86c24b10038cbb4fe9f897e1145b2f58cd3e9120f9a5620f38aa1e1f63906f557ff4a4c3223f5bb13dca34f8a1c6419e24ea57d114c62fec6fb9eee58a16b9e6a6bd930aa6fedcfc591311250e7167d43cca5916d5beead27":"9d156414acb63d11cb34870b937c837d":"":"96abd56d2f8aefe6c687f035df46c3f952a9933b8a51698e47d973b7d47c65ca3ba2474cb419c84a4c3cefb49e78cee1443a8fbbdaaecf73e9059ef34ac5a0df3fc152ecde2286da8840ad4617fd6ebc1e126314204bdc0a17b958430eb9f727498ff1db17aabbdaf43acca0945342d2ba9346da5373b2372b3081605e895c99":96:"3d998e5be9df433da001a686":0

AES-GCM
NIST Validation (AES-256,128,1024,0,64) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"1054d48d52693d2797c80d3f10509d1c808f36a4d65e8fd968e5d56239f856bc":"a708e9d2d27ed4228e5b23d358561a77d684d855db9827be2bc102f2278f1961d3f056fb76f76204b2c96b916eb5e407f98e58edfed06de2388521832d97211d851d3e29658df738e3a15593b9db016d9e46fe9df98ce972d59f7058d484886ffaec7b9fd973c55644831241c1ce85bb478e83ccefd26b9718bfe910ac311ecc":"87611b936873b63abeaea990d6637a22":"":"94473e84659bc18eddcebe3112f55426f48ca4d670291fdedd42cc15a7415aa6795fb75b39434884eb266677e1fa7f530c6f3aaa733c0d9c06291bd7dff4c4e5857b2ee9e9f1f61a85571ad32dc9a3259017abe9eb5111e56df2913535669f3b2d722bd35fcdbd6541918885d9677cccaa902b9d3599cd4f0df1f35f4d11b8cf":64:"9bd7cfe1023448ac":0

AES-GCM
NIST Validation (AES-256,128,1024,0,64) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"a95dc5127b9cb1c82d558d5b24ae049e24447fd676a49350089951afe01dc797":"45f81fa4780a256c40a0efec9547310406904d8991bcf964aa35ec9af457e2a642c1343827839f1f4b42f2b226da351731f416a4b4151f07927c278b371404f027bb2058e1765b367f5433a43fa4153883351041db3f066ef284a3eabd584d1d0b1d594b4ce7b5bca1708fbc661d95a9ac0d77dc29547f022eedc582fc7158c3":"0b177d01993ec726fff082ec88c64a31":"":"16c77b7f541d2dc4e8d31da23e04f18f4254aa283e8cee5b776f3d9a27584f459d0747955efff8945f807209ddaa6421846647d4198534b244498fe13a9073d372171d1b2fc38af66204f3de04000c093ebe659173b8d78dcfb8ca9003d2cd44ed168e6aaf55a06f29e83ceb32b98bafb59f109599f88b5c0f0557bd2b28f03f":64:"19eb5f808d65989d":0

AES-GCM NIST Validation (AES-256,128,1024,0,64) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"53d6393dd7ecc40f2d52460ecdb0607133ad843ef53f380cd3a2755bfa567abe":"72199c54dd5efb28c104e3b7210855506f6577d15c4eccdaa6a621a572e15f5845d648cf71b9fafef3411f6c1a664c7974fe71126a5cbab907e2caa342d8d7a05bc68a72c824896ec40e520e90b704dea441d22c5918f98803a88293384f64f92f11650c2cf4d3b062d30e14d149160742f59a473faf8fe00f4bdab9128c3281":"db7e93da21f0c9840c54c56e9c6ceba3":"":"5e83f559fa54926b731334f815783914530bbcc472d4bbd5e65908fb1c421442cb4c57329f2e4ba3d146a6499f34d8f1ec6d43e0cf98bdba923f404b914700edb235b08b0330097ea4162fd0baa1b7177ef0b29d5a6689bc56b8f975d6b6067ade4b8baf1d47a2eeb5b2ed28ebeded381d55d280cb2fb65ce4d82b69cce0594d":64:"4e65dde857a0f5c7":0

AES-GCM

NIST Validation (AES-256,128,1024,0,32) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"aa4a53c7764a254b06e1d8003810300b70f5729306effba9fb6210f97648a499":"19f3a8c298478d6868bf3b31785eb62e844c37200672e6ef1ecc05c616d981e02c333dbc3f86dbb7ab9ba40e9e57e133e6d1d595fcc6d8e9886a84517212669d5d7ce0f1383cb58681b92dc180c06caa1a7ac1ec974dcd7f2bca7ad2ab2789c9a3a487d64c484319bffa56d854a6d40c62b02d0c7898f641f106ff50d22a12e7":"c32288f97af9b6e31aa7e40d9ef8d016":"":"1fa6aec7a28767c8961363dc4264e6ab97014264f6fe1dda7e9db8646ce9a5463f69e91aad2fce696f9b641d75635bfb0f97ed2d7beaca944cf8bd9dbfffe77b5ae9fd032575e5333c7ce27538c609922843de87b960ebca7c2a2ef9702dd0c32f787b4d7df248fdf526d594a90bad0d6a8dffe212246c36db71e2d348326624":32:"1699444e":0

AES-GCM
NIST Validation (AES-256,128,1024,0,32) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"f420b6ef96d9bfe46dcf18246ee230790a6fc854e730f1dd2d1ffd0e8b5c4776":"658a954d6c61d0d6f0e81a3c1cc65684483fdc95f280b6d4c964358596c25ca41c389932d74a1a3a17d041e89b7110ea315fadb3128c2c469c350bf9b4723aa9c8abd9065ebbd12c317bfb7090f09633f8c1184f0c4fbe10f5486dbfb847536c886f7d144ed07272a7e62fb523a04111e5ea9e1ab415fd17e72143006db14e9e":"4982f502a37eea8bcf316ced466c9fb1":"":"8630aa78aabe35d9360a44bb2094209b6f70d46d71e3949803cf54e33dafd54c6e49eda9e26dc5c0c1e34908f5281c8cb2a1aeee81186cf45d3eb22f486320c7ee0fb7bf3c211b232a8426e7e82f3e05881bf7d9454cddec7f28e5358cd0e9ea2e9cff938be044c1b21911d50b2ae23ab1aef377511ea657adcb560c34209f8b":32:"3aa91b73":0

AES-GCM
NIST Validation (AES-256,128,1024,0,32) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"50f3b822dfc70382d8695811e6b0a2896ea2bcd4d5268778cd484053c8a19288":"15bfb3a562ced63c92561a78374af40c88a08ce02392419e03d7543365c5b6525951ef2dec5927474a0ef85f519e5ef795881db3eafa765ec38e6be7b565a878c13d90c02889dc50cbe87081d9225a515504c7be15bf97f5d72a4d81f218a148a46fbd42983ab002fce0a54719bfe301bb761753cb330dc25be517b87d0428d9":"980810c11abd3aff43408ec9a69abcb3":"":"12632296f27eb2439009f6032a3f648370303dcebaac311b684de2496f399b271347b19e045c1060802f3f742b6c780d20b9d589cc082d7d0d580dfb7231171cfb612227fcdee7feae4f8defd34c89fb0d68570e782192a7bdd9a5464f35dc6a4282cf9cc3fdfac988d129eddf8e0795ccc24a113f872ada88834c974df8bc69":32:"32c1c4c5":0

AES-GCM NIST Validation (AES-256,128,1024,1024,128) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"29072ab5bad2c1425ca8dd0ae56f27e93f8d26b320b08f77b8bd3fa9d03edc6c":"3c7afc5cfc5a1e141587e93fef8427d4f21d892b983b7c9b6e9de3ee168837a1533847c8a2e2ab0706ac1474e9aa54ab57e7860bca9ebb83bd6d3ae26ca5387abdb9a60c4a9928484742a91294b13ab8f51eb4f599a30e9cb1894aca32a62a4c2793ee6793df473f43234c9eafb44d585a7d92a50aebef80c73c86ef67f5b5a4":"0201edf80475d2f969a90848f639528c":"4c8ff3edeaa68e47bbc8724b37822216d42e2669ca127da14b7b488fde31a49c7d357fb9aecc1991b3c6f63a4ce43959a22de70545e6aee8674d812ecaaef93ad03b5d4c99bdef6d52f21fc7fdbeb1c5629a76df59620aaefda81a8e73cebe4c646beffd7f4a98a5283cc7bc5e78b2a70f43e0cab0b7772e03a5f048ec75081a":"f3755aae6813e4e4b84a089ca1496564676655ba3c94e59c5f682adbbfed21e76aed0db78390258cf5fbf15f06c6b6468414cb6493c8b9b953b4954ecaf07ecaf8586ae001710d4069da6d21810bcdcbb831f7041cdbb984b7c55878598a6658883178dcc0fa03394519b8b9c3bed0e5c073429f5dd071a9184b015cbbbc62e1":128:"0549dd9f2a123bd6d58e5cd16c0624a1":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,128)

#1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"aa9999af53720d0c1288fd3fe307a471160635287eebf41dd7
7c82d1f9cc9d61":"6ce6f2dc202750219e15a24e1ff0678ffdde55b27cdcab6da188bd5235a3bdc677f72f106579d02c2
970d4542e4e2372886e1a6d74c596ce735f51f2ee6aff4d62bd24112ec7cd1adc7c660561f163170cdf047c241c53b8a5
b2e03fde48c249a319bb90c2693c468c9dd136e94e05f067cd1d68244ce50be318ae0464b79acd":"6299d651a032bdf3
a7e6b25ace660e30":"afab0a3d1960ac973ee2f4461dacd10d189412b37e572cad7888bb4d2453f1eefbd6725aadd5f98
2393dfa59c3cf1ee342dd91e1fbfab10a802e3a0eda226fde2686e7db1015405a3d33c921e5aa857bfda53ca3aed3ff0e18
c289406740a7c5d9f86ce43db40c9032e98ab126c7c0364e2efc008312b7641d36503d183fa5a5":"a8059fe6ff711616a
fb591b5e5de497b3b7813f9de658c7b47cc3e7b07d0805c1ba05856d98341869b8394f3b5df2876ae19837edb3931eeb
eb0f26eb6c4a2ea78003d82a98111305208ccaceaf77e5d71996cca4f9a5eb712dd916b71455f741ec2dde51f56828667
b7a2da015e1886fba71e496a542d94a38efbcb5353fb89":128:"2ff4d8d00400ad63a6ae7842eefb16eb":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,128) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"31721e5e3a748a7f7369f3dffc1cbb570ceac868ef9d1f29b94
4b7e86a26d273":"6afc1d22233a60c3e6851447de89152a0dbadcd87e35fc947ca4bc886f1f87549ea106b097e265513
6833d06dfb879a85732298860c149c5e5ff03bb2a95d9cd3deeb8ffdf951ea5f97e32c1ed75271d2ea58d158ae6d568bf1
97d69130977e330ebfef33f222bfd5b56bc6b0382dc99c4f0e42b0aa7a117b43f96d43f6e02dd":"523247d56cc67c752b
20eab7a28f85fe":"11eb41aeae3611f0de77bfa1221ef5b7d254faf893dbdaead926a61605f8a86f20f1fb84e0c5acd1951
43bc5a4f297bf729129f898a2013175b3db7004115a6120134d8e354afe36699a6c6618d739c805b5b91739df67de766
7729f1d6eae1a0609897999d474be4d8b826df901c6f39d522570d38d2d1aa828382932a177b1":"39e7f32bb3e8436d
97a1d86a22750768001fe3a805516d3f800352323afd221991105d12da69ce7430402fa7923958ad5ed85506b968c4dd
89516d6e3d02e722db3954ce098ec3299ef4f2ed4a89f383408dceca9dabc6f8eefe5a1f80093961c29a94b222d1a04d2c
1e453d2e02977f3dd77a4659e2bde2fdbba8e2829db4f1":128:"506883db674fa0417e0832efc040227c":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,120) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"100bd2bf9c8b24cc2e8d57697cd131c846b55ad6ff0b214c0d
e14104b465b58b":"81c3370da989f774c1962f60c57299747481bea0e6b91df846e6ef93cada977bc742ee33ce085ae3
3eb9f7393a0943b647205a7e1ffb2a6a803a1ce7a88902456d66612362962b97c7152b57f1d54de94a39f07c1a8098da4
ea5e498d426b7036c642fbeebefda50b8c421a7a33b1a8499dc35011d80a51d34285824d6f01722":"363e8af6f38307ec
126e466e7056cc45":"471f7e9a0b505b12996747ec9e32731f11911ee95d70795bbd1bba34cf782d4100ce30a85b23f9
f817f30e8f314e1a23e101201c920ce12ce732cc3fe01c74a9ee8d3e1599aa22f2398c3265d4dbda626a8ff4262889009e
087fbef6babe33d7300e5cfc4c0056f3562a913d2594fee8e44959cf728599a9d3e7ee4a9ecd6694":"9494d01966ac887
b8295bde61f0e7d006ea7b5c984a29cf5d849194f35d7b0f6ddb3bbd9646d7b9b961c515179901d2b04cb7cf7b6c8736
d1d472ae8bb9a6dc9194b03b3f5373551a5ae0c0f023967669c873f0acfb02c0ae3a384e70f7a7ca05861f257f36a2ad5f
bb591473dfc3ae1264dca0e889e0ddbf93dadf75db2059b":120:"5c78d914cac78c514e275a244d0ea4":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,120) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"614dd1762deb5c726eadf0e6587f9f38fa63d16bca19269554
04f1b9f83e241a":"1ae828a1693d3c24651ab8ba59fb1185d08e6cc4a964f30dac59cd81ff4bdfce8023ab1b6dffb594a4
250d25f611763efb4152cd35b937ca11373d237f1f8b3c0e21b942beb1f4ffe5014198c9ff59896ddfbb55e69963e3ef6b
03d3fa134977870cd6f3ac10bbf59bdcc9f103cc2d58f294ef5f007a9f903c7bada08cb454e6":"10d079a86894b0c17bfc

c8ffc4ecf7bc":"c4035f80b6d2ea288afd4ddaec1eb232b78be5a86583fa85f791d546102c97ace9716c2702483d762c8e
4eda12f3dd10a9a49a2d72cd4694fa794477b54b4367be6b548675aee4c351e3f66c7e113aecfbcc57b8bbab4a039f284
88237c75313e62612847b915ef9b582e146b2bfabbfce576a984f5ce4be0e6bff5480584fc3":"bf5fb0445aab46aba5048
01d5356455f28c98f300670a731bdd0c901a1d5564aa31f5d467e5f80dadbfeca61d2bf72b570f3935ba04c45a2ff7994b
ac6cabf84db2a42cd5db2a4f160c97c76817cc5cb62d4006d895fcdb218c1464b5caaadbd1f61779938e9a84440615eae
050cd6f1713cfbd695d78818b2af78157339e9d9":120:"6d815ee12813875ce74e3aed3c7b73":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,120) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"12e97fafff7d397ea34efc0a8528afcd51c1b2ccda680ae9049e
dc8359b78ec0":"9fbf0141cd50bd1b3ccaf137b808b698570642ab20c32120901622b34173d7ad119abca3c61bbf1e6d
d5cb182a079f3e01b0e5263d984c6186f01792125dd6c47c30033008ca2e0377f990285094f652c55a348242dfaa59f76
989fcf86033c8d9c0b2a526bf46cca207e055e1dbc7cf3d0b7a840c8fb5f85784c9e4563f71de":"8eb11abfe350c0d5a6b
02477b44867e9":"0a830029d450e20aaef484d4abee9dadeabbd6feaf800b3a693b4746db059efb7d110405b45e45a9e
5acf90957c154674dfb2c1cd787af371e01bafc4e8475d0268b969d25756a1121a519afa61f3d6ecded4e0640f0ddd471f
5b8e82029fd2887df4e65af9580390b6924022e39acfede7530e5f0e54f0285ba565ff49af542":"067cd6ff8461ac80217
ef70a91dcf6edb2fbdd31856815cf356fffa63ba3f5cb293d7f1ed32ae40248693617f27839a34e871fdde635c04d1e6674
3f730a06e2be25cafe1d67d804879fe38e009268ec50a0294da445c795742ff1e924170e4c2e0e9ef3bdc26c251f553721
8d295d93d57baccc4dee6185c235d7ec5c9926a6":120:"931f44f10993c836e534a59c1aeb98":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,112) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"c732da000262de558bd3ea65e66e20e11605170c90b67708b
da43f40abed74fe":"7d6c981c30ef87a46f53aecb4c97124fb94b45057635d5bf1d4f3a3bdb534e9ab62b4a425de9dc52
537575ed9ff406cfbf75403d3d9cdbd9fcd520d62065f81483427fa27964642cc1a07822da0f6234a689eb30e8425d770
9abfd18666c76c963eecef20503ee77c96802c120abea1428cc64a08fc20860527854fecc571a6c":"523dd34ea263c31c
2215053986626d02":"f170556ac5d38f0661bae33e0826356c8488218903eba1bfa49b16882537ef78283fd9351f37f4
4a7687049a608c3ddcc82817d4ba96a40d05807a38ee3f2d5cb8b1121db61318fe22bfd3afb319e84c4e2f94570a92433
db29bd2193485449c719a2c6030696f53ac729df90678eb018783b25740d806d1ef6980e10d396595":"3470d4544f7b
fa3ac0627a56e66c56fa062188440834b9238bd20e89dfc701fe6cfe0bf4ea2387014bd83c63ab7c912e1c0dce7c2d92ea
ea155f886b574bc94a8f4f275dffe2d84173a05b99d8029c36dd3c35c12709d33f55c3bcd96e9a815f77a4fe8e50639d8f
195a526486f1209d7bf7e86ac3dfc4a1d2cbddb6d330e5db":112:"5924f3ceff0207fc8ba8179a9925":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,112) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"2684bccf2b845314a0c4b8b5a780f91aa7ed1177539122dc87
17c14bb50e2dff":"1a4174d4e18ae0b6434f35dcd9c86cf158c42ce00ceb12f4356ec118d659820518c326a1b2ab92279
d949f74c45219c660cb84fb6b10b14d56a501173fd3b129ac89db0de22874d92bec724e94751f91a817a42a28e8e1567
2172c0b0db4ead46b14d4bc21ad8f5ba1f9e7e0fcc867700681349b8102a208d76ae4ef7df5b56e":"8433b59b41fe0cdc
5b30e4e87c5028ec":"280026eeebf05e26e84955e4a36352d4f97f3193dce0795d526d05645bf5d2eec4b92ee8dce54d7
8fd3fc3e36bc79d5bf9ee3b2699310a75dbc5007bdacb4dc88d06515995f8f5b1aa90cb8fc036b763a5e819db70c09180
2fb7f24b9c2a68ff194032fffc4ef798936aabccbb43f22a2bbd7e1ab9d0434d443dac4929b84193":"cc155e04472c0872
d5ccf8910d34496f380954da7653a1e1d3c460fbbc791c9b82e35176e938b7e21eb4690ed9fca74ba45a03dac4abc4f62
5ffdfad02e1acccf18b5a1878f911fb6f6e09ce0d4c6a0bb87226e914879a1b3085c30e8328aa6e0d1c49c21b760b82e46
9981b40ea102f3998c81dd9799f484ab89b19396ab7e1":112:"5a80008e6da40c71b316b84ae284":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,112) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"484a33ba0b97c2887a86a1476f274e236eb37a72e05f9e74348248877ea99e98":"4d81cec14b398257a31ad1e3581c00d05e12b37b71260bdd95bc0b6981b614598ffbbb3ec4bb7deb5673a1020139877122f88504c9c53265706fe76623a9b488a3dfdd4cbc1b7b46c7fce9d7378e164964c0a377337a5c172e5e4de6206375164cd7beb0305d7a90f5c73e12f445326e1bc9ac5acd1bd4bcbe4662524891a2e9":"c3a5cc19aef6d64b656d66fad697b829":"30f276f96a50e17b452dcb5e1b4ab666dc7c4c72d0d9ab2abaf77eae2e3bab7dbe5ac005d7eac5480e1bae13646b59155528abdc148b3b71f06d017c4b12d64aa3990cc96941eaac14b60eb347e0be873de2b6fe2b86e2c2fc063b29511b70144ecd315b9491001b122701b9c8cc1d85427b6c60663ccd9d1fa84e1c2f609f36":"579fd8fb50d795b5b208c2d5b0a8b1804f754a30a1003025301655aebcda2d2ff30d29a16d0fb17a28401127750fc87c9e3aa08540817228b049c387253ea2359035b8063ab4bf54504ca5ad93b54b8ac5bd0c1ef3c6769fb1ed239bb76f3e0bc51d356aa91b494d22749c8e4cdb1629e93f7c6e46ff9145916c1275669ae5ba":112:"1c39aac1d5ffe7916a08ab2ce279":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,104) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"4a5f5321b515cfcde493148ee4c44c693b1979b3a3ba522a2a80e5d27c93fd1b":"962b8504feb57ae73e93c2e8962c9562f409c908e51f9904df1623eaa0c6b998db6ee8919d805b6ffcc37da51300c1ae16bca21f8f6f63af989a813ae8fe28c3fb012f003dab7e71b08d757799208806062d62b4ac937712409f9fafff3e3579a4d92d4437a6f0b263e1da7e4651e0a521be5f6f49ff5a0778f07bd5d3dac696":"c2cb0166046bad0cf0a107af83921d7a":"e48abfb657ab33f58eeda8c58a20e7e299bc3e7481f704c326529408580f9a5130cf6f7368502d20b03ba6c3b8f6f28c076a3ef7b8e987750dc972be953e712483e6f328da57e4b5c501fa7c720593eb89ff9644fbdc45478f80ee89f096694dcb44a9b3a6aca0904d4aa4e475b4b24771df9fd6ef9557f4f5c842ac241b212f":"11bd55d969603ff3d46355cb19c69557b99825a4c23eeafc8eed8422dab537c0fa9753191c49a6fd9e0d6760ed816a49e7f5704b5936a498544e2bbba7875c513c031f11527ca1b9b579960be6964fba9119dcece8205c174be07ebffada83375678de76fc012b0ee179787b4aa9fb6e2b459575260eb01f23786dc24d1d45ef":104:"36853a029b5163ca76c72d4fec":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,104) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"c8f7b7e6295fc8e33740bf2807caeaf4b90817cc3ef3d9f38f704d9f6164e41d":"4c26e489069b487ce9dc0e295d5e897604011853740 41b0efca5bbf758e7d010ccbfe5999e2a817776aa8f49c1e5d43bcdade2989fe5be635dab54cb0e390a21b832b30f688857b9e09c346bcc5397e51cf71acbe1bfcaa1ecd7e87fe5dfde180d951922e60dd8203ff210c995eb54bb981f7e931f0b1f52dce0cf1b2eba503f":"903b2eeb9d0b3794acb7439d341cfe0d":"83e99497bfbe9393b065b0b18c13f99b67f1fdd724fd5d70cdccd2b8dd658499cb9f57e1a1fe39634ab0869182de085722a79eaabf057aac7b3f3230f51a2f9b48b49d592f02246dacbe915ff9d9a53f7e5332f7a9d89649050b075c07e5e74f281ca1a0dbe632c0aecf3b1911cd6ec4f8facc2777d0d14784bf5951a1c62c33":"63e2941bf4a13374627be66bdd4e57119149f81f4c1a8a321d27a4a79e7d61e2dcec9d7b13fcccf12f5b059cc209f8414ae81966462a266e92b4b3c25198ee240e0bc6f6197df1e24e8d4379fcae89e6240a7f9c7bab886e79990b846e98e4bacb8b3b17422249943e9973de42da5e38e4eb52830b1facce766b3389a5312476":104:"6e31c5db3146ae45ef5d50485e":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,104) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"dec062efc1bd2556b87a81143d025abbaa532c586d5ebb065859a2071f8f07e4":"02191bcb060e61827dbddac6c2961dbab8812cdc2ac77bf0275628e8e36bae18ad4deb77b2682ade

0aef76afd4592173ba29dae4d0735963c803856eaa6f60a6c21785358e87f3c4a91e321c59e04c150297de873679194ba
5ca857f7d91ffc358e73810d555ebd4dbd1fe4fbc4ffa4ff38e4b41db9af0a84fe9828708631469":"19abd0361443c3ac2
a46f2606eeb1a69":"c3785e7c0095726fd1f3ca842057b0ea2baf9c3fe1119c2147609158a2039f26cedf8a44e046955ba
7e7cad9f48cb49274fc53b109d7897e080af252e7dc64807c276bcf668d2cd505c9ce8e584609d293ebd2a4515bfbaf78
c413d6e29dc90974db38b564ffe9a40d3955dba9f19b6f39bf942669cf80e4676d6c10df566ca1":"91a16c7fe029e3fdda
cf0809dde7d041c438977b89192e6fed7605d0133f3d9e810355d186432f6529bd2c4cb9dadb4fedf5128cb45e25a3a46
bf74ed93f31349f64a69dbe86592d76e437947f1c1d7270d1cffe80afe10ae8523541961eacee1838c168a2ab76703ea46
74a68a96b8a298a672ffc140e98e452d501fd57f000":104:"5b4071a4be0543aaa59b56de35":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,96) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"9b7b700d978e33ae9311b206347f488e2832fad5ce7e6026ad
5e24fb47104fcb":"37aef6e4200c6abc3d161daaf9dd6ede002ce8c63d9ed54e8ac56bdc8d36906bea663d2857d8d5431
66ba150827735ec78e37f92e682275e268d377b1880970df232162e55c9311882f889e7d183e5cf4972691c85f81c47e
1224b9c97ee3963d75c6a032270ad6d713c999913f0b58a2d4f42b85a3b0b40541a31398cdfb4b0":"d0bbc284af767af
9a31b863d66cb6138":"dfb87a65ab2d99d7d753042aa47448ad830e546d298d6ad52b85207bbb0cbe8cf3cdb12b3544
f1fc228fdae04a241abf9e71de8ae14f2de2c261469c383c682e13582e07cddb1ed9bff1fd2aa0be7978096a914676dfbe7
bec6edd927362f656ce1de86229bc511cfec4cda77a1e761e7ab8664e4df08cb820ebdb604c2cdbb0":"dcd5575d94fffc
647d4c081e3ce03928651419a32ada2af02de2f58d68fa98eb1fd5ef671875719a9c65b9ecc69513408a79a0a5d57cabd
04f8e651f5b8fc1ff42ce58d8a212ac2bcb83c5c53c542c282553a62b4e3d7d4f049ab13172739a0f46e0a2fd9aec54eb0
c84141c6b341783754372df69d39e48cc24eb3d9ddb21a9":96:"4a7ac79db94b27469b92343a":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,96) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"ce15e61edd9320ceacbf3984d87c707159caa738e7e76285be
00b5a95954b523":"8af4a7d92441ce931815fa4e24d69f66256fec7e62f79a029b684b5db304a46b2a3d3a7ee8d6b7ae3
8caa7de526d5c0f28dc65a0913a383b7ee1640cbe24997ba95b9b12fa1e9ce9f9100d883c16b6286dce17e381af15113f
56197c97fe6b45be00a3df05045f476829d7b303211ac97cf989a18c16e27fbf23570d9d18f04b":"b1269c8495ea1469f
f41d8154ae6765e":"0ad26a08a5cc2ec825347d7ffd5aac795eb68aa7e22970d991c863fa6d1fa720137aa5cde4e38262
5a0038e6ed72da3b5003c1b2a953c2b2138e0cf870cca4afb595c0451aa793fb0a2bc43834a0aca1e760590cca765ad67
2ead975993f82ae6765c5afbddc6062d7c4babebf650ab097db1a1d9a2a99e8fd2e0eb8a7b916f6":"ad0ab4e77257866e
4a57cf44fa4049428e56a6e8b8fd47b4cd00bfce84fa8f5a43f1df2061b0a37311b4a1436bad0d61d52ced5e262ed41a7e
b125d61cec2e3fbaa95e533b43f318048096ebc8466f0cd609bb5e7c3fc6e5701aace546618a170f88c0b7ed76b63759c
a4e4b931a86ac379dd12ad2cba7d47a19a3ae7c242fb0":96:"fb1e988f9c97358a17e35e6f":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,96) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"aef24b8205d4085d978505f04724293c2819ef9f3f03a6c758
078690fc4bf7c8":"db26453170db2f984312e0cf961d1a7df1154f0525c31f166be5c9f516736501f9f2dd8096a69b644
1888ce27aaceacb0b365a38e4e01e2e34027c023206e814f22d46fd2fa69f87509ddced4b8852a76b2532b92f069b8c92
2ac13b2b7f19cb7c524657a4ee6e989cf2598bef674aa31576776853fb7f9a2704d6b3ee7fbcbb":"81456baa337c3dfd1
62d9c5f72a2e216":"484a5f4772643cf74ccdced0e5d80862f9300f26ae3139968649d3d7bb761b313f2ba63798b2040
d397c3d1569285fee8498fd9254851c15b98af5bd351fa72e7d574c62ede0d728e1279e8b4e4784fd63ea7851e99d1d23
56bcbf868528f8d0a90fc3b884ece631648d916ec97abadca1b0dd7670e6ad42245021570582ec7c":"da95c61cd2bb88
fea78c059c254d2b949d4fc291c73ac178ace44c1e6a339f64931c857d3a7cb276a04993620adb6918dfd3f9083edad38

4a8e6c1d4799d526a1c969d8deb0e2667d6d06f559baf914b49fc463244528aa6522d19699065438d939521d7d7bb14
9835298f2054bcaae6d786f6dde133b640697a3d37c697579a":96:"bc1c1cbcad2e1a66ace079a2":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,64) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"9685aea9aaebbd691e679779034729306d5887bee4c1f90f6e
e3a397a0ff3ece":"ae3b2fa1e209f72c167eb16bc15b7669b87d4ab516e428157810b87a83e90d56e267bd4996522b5b
22c2a349d3765ca27ea27057dd71f7c18ddd053033bd780b6cb689f48c383e9c717b9b265cb9e32c70c4a7d8fb933e98
6d996b5ad914cd645b74c47ac3a0de952ee3fc73ada83d896da7ca0b2a0b10e4f701fa13cba9ec50":"b1bc140531ae8c6
9e2ffc784e0988038":"294ff858fa6efc82ca3be4d05332bbb951a71a7ddfa4b78472e1582b445312eec11793d8d6e1e8
58d9cb078b5fc9083ac8a3e3bd82964cb07c08450567922299f68fd47663c7a77c29f2b5347f229301433d5a75263158
a0d80095859e7e45476b99b23412046bfbe4eafff9f7820ba49919d2c987cf00c286c784e7669d8fe8":"6575128b576e6
8f7b3709e325b3d616783b42ff7f7631eb62b90cb0c8a86bd324756f43af53c33cbdaf9cf64ea94cf1b7fab5003f00c1d0
7f3fc8eb1931d759f9c43477ba22311a111488092c42b7786facf42b861a824cd1bcdc603a77d11253f15206a929a3e16
e8737d080b8e5f0da8896226989a9964d72e491187250472":64:"f78c4dd37c06b197":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,64) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"3adf0da24394a98c7beae01d28f261a9cbd887aeeecc0c29e84
540264d5a6bad":"8cf023d717b0f82f2b81750b53fb665c1c90f4740af4a3534b36b847df33ba5eec19eb24ead70a4b61
3a82572878216181d59b0c4c4df99be08d021cf182724d8ff5ec4e85884d0f69c16238fbbdbc5529ffcc4e418405e4e95
139f79d3115a1ac56820cd39fc413ab72f7d447f947cb0541fc2be261f1246c0a786199013b22":"ad41288817577316df
2d881ac93fcdef":"ad33ce922372fbe3531c0dece69f85f18eb1bbfb09a178403832308de0e54b1010db2636c4b7d9caa
478138f61db5149c9fd7f3b45b7a1876729fe67622a37f0b322ef9cf6043b301a5d4c81e6f347d22bd3e40722059d3be9
45845c6b0629fbcfcaf885c7f393aa81f242c48c61a439574761ef6b671972cac664403250750e":"9d465e9c422832394
6b1261892243d8455edb9eb8633d026d4033fa3965d20730979ba6952c0f6f2c5768f03c19256b64bc759d2e7b92424
bbc668308504ba34384c2bb37baaf91a3a4f0952a050a3d69853141b49e86eda3bf0c4db4ebcd1c41e7f13eca20bf574a
47ec45b8c98def17c0741805bf8f37923ba2b5221428578":64:"507618cec6d03964":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,64) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"9ef64b4132db54668568e2ae66ab61f62a820c7002a67a7e42
006280a373feba":"4b96dce753273188c4cca3386a7415d5d9263757376e1f32797df47992e92e1bc0ab0833363b3acf
fde22602d4e47307bc8f252944414a15e1398693fd3b8bf4d8101cdcf70ce2c9de8cb7f5bb17cd83f09b1bc78ba07c34b
9214e250c5940e9794199cb392309027d5ab4f32b51c533db6732024bd412f2cb0c5178d5296aa5":"07a86dbe2cce04
0eccdad79b3d211ecc":"af7a75748ee293015b600ca82ccc7718f4ecc20c3a2357ee02fb726330a0d79ca8bb97979bc0c
89f4c60d7154f8bd29ba6ec5f2f4be286ea8a258cf6bd39b4f42d6db8e70c99ec3af26bb4d8003dc6fd0fdfbbc620d511d
4d5f09ddf975a1663ac2979ae0978b0bc1e7bfcd660ae4ac7f1a8f6d8ee35752ed59a604f07dfda53":"e3e862146b6fb48
b01ababc462dd560298eea7bfe5f3248e28a908d1de08c7e91fcf63922c394e7a51b64f4382225093e78598c050e588ff4
ad38f3e83dc07b77ce569c6ab8f8a9cb0056b3155aa1503cebeb64c86d6d9cdbb178ea9a01a8ba33a1c48beb92ee4cf60
e7dedf986019e19089cd186c98c229b0ff42c9e1aca571":64:"8614c216055c0660":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,32) #0
depends_on:MBEDTLS_AES_C

gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"f14ac79f35bc5a685433eea5bb7fd69fc959aabda24cbd8b7795fb2e41f90ab0":"8a20da14819079960b77ed5e548d0aa0bdcffb752817c1abe4195e612cfbb58c8e5a8af69f75bad10ee8afdf0b0d5c46c4dc11c32bff16d5e7e82e77fd80e475c6a5a0be36718af232697ab22314306b8ee32484b3461da657710c06170e80a6a8844f898c2be29366c8430f2392d100ffd419603cbce406dc7315577e6e9ee2":"353e1d08edce44c966430513cb7a0383":"cb1dde4ff5a6867038c170192fc2d292f5bb349d5b9a903cf3d88c09ce78fb1f4a776ff7588a25abb5e5f6a44791d7296afef3f32ed31db1def37dd25be0570a204955121f9c65b79a3ea88fc452dbcb82719243c11bc27e3408adf802b6e8b4e701ee4e9dfd140cb3277bf605bd5fb757d2325f7805fc6f0d1ea5a6207fac5f":"49b5e4ea0421034c074cde67dd39a0310c3f31e8138672ba2ecc0777be542f1c6529836d5206b79dac83d96aab56787a35c584b31228f007f11630328c3f40a57be37487689ee5babb576e7d14ff0f1f1ba6e4be11637352a4336327681058b99df2e44f9772de4e0e456d2e34dec5eeb335b238e862841d166e0612cc0f18f3":32:"88aed643":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,32) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"b55ac909e73989e310ae37d13c54bbd5a126f419a3b01a2ad8961d89bd247f81":"8a663e8b21a027c4a9545d145d42d9c67b4fcd5d0e39aa68822aedbd609e2c681f60e6315035321de739858b2b082bc05551fe9b8456c2e89c6151282c6068b915eae5762e4d6d765d667de58a315e061b3d60035ada50f59258eb6e2a1cd6b52eea7eb9d404fd96e71f19feff65b74a4b4f07061adf7c1b0e54e2ece7a2cd49":"9328abab0d3f63c75ddafd8559d96b4f":"cbae20aa1996abb62471aac91cd78080953fbe3b165d4c9435832ef1106e7e3424db8850f44a431c289ab4f2bbbea9e5c0c7aaf2e8de69c0ced176283662cadd280d8fda0c859551f0f90893ca57695c95803a1546826922ac78703d7ccae285b7ccd4bbab551756cccc6869dcf34b6af8d8b80c25c6fb1d2caa7f28161fb854":"457e13ff4eeaaae75d14bbf1bff91706c3168b9b146aed29dbe31b12ad90c1c158833be95701229ac6e4a13997e0a2d961d4a0021c4d8920ec54a9a935e5ea73b17e8fa60559df76bd07d966dfa7d86d1a77a313228b2ae7f66b5b696726c02af2c808bf75e0b9591a220e762f57c680ca68f20b2b5413b07731bbd49de039bf":32:"5de0434a":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,32) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"1477e189fb3546efac5cc144f25e132ffd0081be76e912e25cbce7ad63f1c2c4":"7bd3ea956f4b938ebe83ef9a75ddbda16717e924dd4e45202560bf5f0cffbffcdd23be3ae08ff30503d698ed08568ff6b3f6b9fdc9ea79c8e53a838cc8566a8b52ce7c21b2b067e778925a066c970a6c37b8a6cfc53145f24bf698c352078a7f0409b53196e00c619237454c190b970842bb6629c0def7f166d19565127cbce0":"c109f35893aff139db8ed51c85fee237":"8f7f9f71a4b2bb0aaf55fced4eb43c57415526162070919b5f8c08904942181820d5847dfd54d9ba707c5e893a888d5a38d0130f7f52c1f638b0119cf7bc5f2b68f51ff5168802e561dff2cf9c5310011c809eba002b2fa348718e8a5cb732056273cc7d01cce5f5837ab0b09b6c4c5321a7f30a3a3cd21f29da79fce3f3728b":"7841e3d78746f07e5614233df7175931e3c257e09ebd7b78545fae484d835ffe3db3825d3aa1e5cc1541fe6cac90769dc5aaeded0c148b5b4f397990eb34b39ee7881804e5a66ccc8d4afe907948780c4e646cc26479e1da874394cb3537a8f303e0aa13bd3cc36f6cc40438bcd41ef8b6a1cdee425175dcd17ee62611d09b02":32:"cb13ce59":0

AES-GCM
Bad IV (AES-256,128,0,0,32) #0
depends_on:MBEDTLS_AES_C
gcm_bad_parameters:MBEDTLS_CIPHER_ID_AES:MBEDTLS_GCM_DECRYPT:"ca264e7caecad56ee31c8bf8dde9592f753a6299e76c60ac1e93cff3b3de8ce9":"":"":"":32:MBEDTLS_ERR_GCM_BAD_INPUT

AES-GCM Selftest
depends_on:MBEDTLS_AES_C
gcm_selftest:

AES_DECRYPT MBEDTLS_AES_DECRYPT
AES_ENCRYPT MBEDTLS_AES_ENCRYPT
ASN1_BIT_STRING MBEDTLS_ASN1_BIT_STRING
ASN1_BMP_STRING MBEDTLS_ASN1_BMP_STRING
ASN1_BOOLEAN MBEDTLS_ASN1_BOOLEAN
ASN1_CHK_ADD MBEDTLS_ASN1_CHK_ADD
ASN1_CONSTRUCTED MBEDTLS_ASN1_CONSTRUCTED
ASN1_CONTEXT_SPECIFIC MBEDTLS_ASN1_CONTEXT_SPECIFIC
ASN1_GENERALIZED_TIME MBEDTLS_ASN1_GENERALIZED_TIME
ASN1_IA5_STRING MBEDTLS_ASN1_IA5_STRING
ASN1_INTEGER MBEDTLS_ASN1_INTEGER
ASN1_NULL MBEDTLS_ASN1_NULL
ASN1_OCTET_STRING MBEDTLS_ASN1_OCTET_STRING
ASN1_OID MBEDTLS_ASN1_OID
ASN1_PRIMITIVE MBEDTLS_ASN1_PRIMITIVE
ASN1_PRINTABLE_STRING MBEDTLS_ASN1_PRINTABLE_STRING
ASN1_SEQUENCE MBEDTLS_ASN1_SEQUENCE
ASN1_SET MBEDTLS_ASN1_SET
ASN1_T61_STRING MBEDTLS_ASN1_T61_STRING
ASN1_UNIVERSAL_STRING MBEDTLS_ASN1_UNIVERSAL_STRING
ASN1_UTC_TIME MBEDTLS_ASN1_UTC_TIME
ASN1_UTF8_STRING MBEDTLS_ASN1_UTF8_STRING
BADCERT_CN_MISMATCH MBEDTLS_X509_BADCERT_CN_MISMATCH
BADCERT_EXPIRED MBEDTLS_X509_BADCERT_EXPIRED
BADCERT_EXT_KEY_USAGE MBEDTLS_X509_BADCERT_EXT_KEY_USAGE
BADCERT_FUTURE
MBEDTLS_X509_BADCERT_FUTURE
BADCERT_KEY_USAGE MBEDTLS_X509_BADCERT_KEY_USAGE
BADCERT_MISSING MBEDTLS_X509_BADCERT_MISSING
BADCERT_NOT_TRUSTED MBEDTLS_X509_BADCERT_NOT_TRUSTED
BADCERT_NS_CERT_TYPE MBEDTLS_X509_BADCERT_NS_CERT_TYPE
BADCERT_OTHER MBEDTLS_X509_BADCERT_OTHER
BADCERT_REVOKED MBEDTLS_X509_BADCERT_REVOKED
BADCERT_SKIP_VERIFY MBEDTLS_X509_BADCERT_SKIP_VERIFY
BADCRL_EXPIRED MBEDTLS_X509_BADCRL_EXPIRED
BADCRL_FUTURE MBEDTLS_X509_BADCRL_FUTURE
BADCRL_NOT_TRUSTED MBEDTLS_X509_BADCRL_NOT_TRUSTED
BLOWFISH_BLOCKSIZE MBEDTLS_BLOWFISH_BLOCKSIZE
BLOWFISH_DECRYPT MBEDTLS_BLOWFISH_DECRYPT
BLOWFISH_ENCRYPT MBEDTLS_BLOWFISH_ENCRYPT
BLOWFISH_MAX_KEY MBEDTLS_BLOWFISH_MAX_KEY_BITS
BLOWFISH_MIN_KEY MBEDTLS_BLOWFISH_MIN_KEY_BITS
BLOWFISH_ROUNDS MBEDTLS_BLOWFISH_ROUNDS
CAMELLIA_DECRYPT MBEDTLS_CAMELLIA_DECRYPT
CAMELLIA_ENCRYPT MBEDTLS_CAMELLIA_ENCRYPT
COLLECT_SIZE MBEDTLS_HAVEGE_COLLECT_SIZE
CTR_DRBG_BLOCKSIZE MBEDTLS_CTR_DRBG_BLOCKSIZE
CTR_DRBG_ENTROPY_LEN MBEDTLS_CTR_DRBG_ENTROPY_LEN

CTR_DRBG_KEYBITS
MBEDTLS_CTR_DRBG_KEYBITS
CTR_DRBG_KEYSIZE MBEDTLS_CTR_DRBG_KEYSIZE
CTR_DRBG_MAX_INPUT MBEDTLS_CTR_DRBG_MAX_INPUT
CTR_DRBG_MAX_REQUEST MBEDTLS_CTR_DRBG_MAX_REQUEST
CTR_DRBG_MAX_SEED_INPUT MBEDTLS_CTR_DRBG_MAX_SEED_INPUT
CTR_DRBG_PR_OFF MBEDTLS_CTR_DRBG_PR_OFF
CTR_DRBG_PR_ON MBEDTLS_CTR_DRBG_PR_ON
CTR_DRBG_RESEED_INTERVAL MBEDTLS_CTR_DRBG_RESEED_INTERVAL
CTR_DRBG_SEEDLEN MBEDTLS_CTR_DRBG_SEEDLEN
DEPRECATED MBEDTLS_DEPRECATED
DES_DECRYPT MBEDTLS_DES_DECRYPT
DES_ENCRYPT MBEDTLS_DES_ENCRYPT
DES_KEY_SIZE MBEDTLS_DES_KEY_SIZE
ENTROPY_BLOCK_SIZE MBEDTLS_ENTROPY_BLOCK_SIZE
ENTROPY_MAX_GATHER MBEDTLS_ENTROPY_MAX_GATHER
ENTROPY_MAX_SEED_SIZE MBEDTLS_ENTROPY_MAX_SEED_SIZE
ENTROPY_MAX_SOURCES MBEDTLS_ENTROPY_MAX_SOURCES
ENTROPY_MIN_HARDCLOCK MBEDTLS_ENTROPY_MIN_HARDCLOCK
ENTROPY_MIN_HAVEGE MBEDTLS_ENTROPY_MIN_HAVEGE
ENTROPY_MIN_PLATFORM MBEDTLS_ENTROPY_MIN_PLATFORM
ENTROPY_SOURCE_MANUAL MBEDTLS_ENTROPY_SOURCE_MANUAL
EXT_AUTHORITY_KEY_IDENTIFIER MBEDTLS_X509_EXT_AUTHORITY_KEY_IDENTIFIER
EXT_BASIC_CONSTRAINTS
MBEDTLS_X509_EXT_BASIC_CONSTRAINTS
EXT_CERTIFICATE_POLICIES MBEDTLS_X509_EXT_CERTIFICATE_POLICIES
EXT_CRL_DISTRIBUTION_POINTS MBEDTLS_X509_EXT_CRL_DISTRIBUTION_POINTS
EXT_EXTENDED_KEY_USAGE MBEDTLS_X509_EXT_EXTENDED_KEY_USAGE
EXT_FRESHEST_CRL MBEDTLS_X509_EXT_FRESHEST_CRL
EXT_INIHIBIT_ANYPOLICY MBEDTLS_X509_EXT_INIHIBIT_ANYPOLICY
EXT_ISSUER_ALT_NAME MBEDTLS_X509_EXT_ISSUER_ALT_NAME
EXT_KEY_USAGE MBEDTLS_X509_EXT_KEY_USAGE
EXT_NAME_CONSTRAINTS MBEDTLS_X509_EXT_NAME_CONSTRAINTS
EXT_NS_CERT_TYPE MBEDTLS_X509_EXT_NS_CERT_TYPE
EXT_POLICY_CONSTRAINTS MBEDTLS_X509_EXT_POLICY_CONSTRAINTS
EXT_POLICY_MAPPINGS MBEDTLS_X509_EXT_POLICY_MAPPINGS
EXT_SUBJECT_ALT_NAME MBEDTLS_X509_EXT_SUBJECT_ALT_NAME
EXT_SUBJECT_DIRECTORY_ATTRS MBEDTLS_X509_EXT_SUBJECT_DIRECTORY_ATTRS
EXT_SUBJECT_KEY_IDENTIFIER MBEDTLS_X509_EXT_SUBJECT_KEY_IDENTIFIER
GCM_DECRYPT MBEDTLS_GCM_DECRYPT
GCM_ENCRYPT MBEDTLS_GCM_ENCRYPT
KU_CRL_SIGN MBEDTLS_X509_KU_CRL_SIGN
KU_DATA_ENCIPHERMENT MBEDTLS_X509_KU_DATA_ENCIPHERMENT
KU_DIGITAL_SIGNATURE
MBEDTLS_X509_KU_DIGITAL_SIGNATURE
KU_KEY_AGREEMENT MBEDTLS_X509_KU_KEY_AGREEMENT
KU_KEY_CERT_SIGN MBEDTLS_X509_KU_KEY_CERT_SIGN
KU_KEY_ENCIPHERMENT MBEDTLS_X509_KU_KEY_ENCIPHERMENT

KU_NON_REPUDIATION MBEDTLS_X509_KU_NON_REPUDIATION
LN_2_DIV_LN_10_SCALE100 MBEDTLS_LN_2_DIV_LN_10_SCALE100
MD_CONTEXT_T_INIT MBEDTLS_MD_CONTEXT_T_INIT
MEMORY_VERIFY_ALLOC MBEDTLS_MEMORY_VERIFY_ALLOC
MEMORY_VERIFY_ALWAYS MBEDTLS_MEMORY_VERIFY_ALWAYS
MEMORY_VERIFY_FREE MBEDTLS_MEMORY_VERIFY_FREE
MEMORY_VERIFY_NONE MBEDTLS_MEMORY_VERIFY_NONE
MPI_CHK MBEDTLS_MPI_CHK
NET_PROTO_TCP MBEDTLS_NET_PROTO_TCP
NET_PROTO_UDP MBEDTLS_NET_PROTO_UDP
NS_CERT_TYPE_EMAIL MBEDTLS_X509_NS_CERT_TYPE_EMAIL
NS_CERT_TYPE_EMAIL_CA MBEDTLS_X509_NS_CERT_TYPE_EMAIL_CA
NS_CERT_TYPE_OBJECT_SIGNING MBEDTLS_X509_NS_CERT_TYPE_OBJECT_SIGNING
NS_CERT_TYPE_OBJECT_SIGNING_CA MBEDTLS_X509_NS_CERT_TYPE_OBJECT_SIGNING_CA
NS_CERT_TYPE_RESERVED MBEDTLS_X509_NS_CERT_TYPE_RESERVED
NS_CERT_TYPE_SSL_CA MBEDTLS_X509_NS_CERT_TYPE_SSL_CA
NS_CERT_TYPE_SSL_CLIENT
MBEDTLS_X509_NS_CERT_TYPE_SSL_CLIENT
NS_CERT_TYPE_SSL_SERVER MBEDTLS_X509_NS_CERT_TYPE_SSL_SERVER
OID_ANSI_X9_62 MBEDTLS_OID_ANSI_X9_62
OID_ANSI_X9_62_FIELD_TYPE MBEDTLS_OID_ANSI_X9_62_FIELD_TYPE
OID_ANSI_X9_62_PRIME_FIELD MBEDTLS_OID_ANSI_X9_62_PRIME_FIELD
OID_ANSI_X9_62_SIG MBEDTLS_OID_ANSI_X9_62_SIG
OID_ANSI_X9_62_SIG_SHA2 MBEDTLS_OID_ANSI_X9_62_SIG_SHA2
OID_ANY_EXTENDED_KEY_USAGE MBEDTLS_OID_ANY_EXTENDED_KEY_USAGE
OID_AT MBEDTLS_OID_AT
OID_AT_CN MBEDTLS_OID_AT_CN
OID_AT_COUNTRY MBEDTLS_OID_AT_COUNTRY
OID_AT_DN_QUALIFIER MBEDTLS_OID_AT_DN_QUALIFIER
OID_AT_GENERATION_QUALIFIER MBEDTLS_OID_AT_GENERATION_QUALIFIER
OID_AT_GIVEN_NAME MBEDTLS_OID_AT_GIVEN_NAME
OID_AT_INITIALS MBEDTLS_OID_AT_INITIALS
OID_AT_LOCALITY MBEDTLS_OID_AT_LOCALITY
OID_AT_ORGANIZATION MBEDTLS_OID_AT_ORGANIZATION
OID_AT_ORG_UNIT MBEDTLS_OID_AT_ORG_UNIT
OID_AT_POSTAL_ADDRESS MBEDTLS_OID_AT_POSTAL_ADDRESS
OID_AT_POSTAL_CODE MBEDTLS_OID_AT_POSTAL_CODE
OID_AT_PSEUDONYM MBEDTLS_OID_AT_PSEUDONYM
OID_AT_SERIAL_NUMBER
MBEDTLS_OID_AT_SERIAL_NUMBER
OID_AT_STATE MBEDTLS_OID_AT_STATE
OID_AT_SUR_NAME MBEDTLS_OID_AT_SUR_NAME
OID_AT_TITLE MBEDTLS_OID_AT_TITLE
OID_AT_UNIQUE_IDENTIFIER MBEDTLS_OID_AT_UNIQUE_IDENTIFIER
OID_AUTHORITY_KEY_IDENTIFIER MBEDTLS_OID_AUTHORITY_KEY_IDENTIFIER
OID_BASIC_CONSTRAINTS MBEDTLS_OID_BASIC_CONSTRAINTS
OID_CERTICOM MBEDTLS_OID_CERTICOM
OID_CERTIFICATE_POLICIES MBEDTLS_OID_CERTIFICATE_POLICIES

OID_CLIENT_AUTH MBEDTLS_OID_CLIENT_AUTH
OID_CMP MBEDTLS_OID_CMP
OID_CODE_SIGNING MBEDTLS_OID_CODE_SIGNING
OID_COUNTRY_US MBEDTLS_OID_COUNTRY_US
OID_CRL_DISTRIBUTION_POINTS MBEDTLS_OID_CRL_DISTRIBUTION_POINTS
OID_CRL_NUMBER MBEDTLS_OID_CRL_NUMBER
OID_DES_CBC MBEDTLS_OID_DES_CBC
OID_DES_EDE3_CBC MBEDTLS_OID_DES_EDE3_CBC
OID_DIGEST_ALG_MD2 MBEDTLS_OID_DIGEST_ALG_MD2
OID_DIGEST_ALG_MD4 MBEDTLS_OID_DIGEST_ALG_MD4
OID_DIGEST_ALG_MD5 MBEDTLS_OID_DIGEST_ALG_MD5
OID_DIGEST_ALG_SHA1 MBEDTLS_OID_DIGEST_ALG_SHA1
OID_DIGEST_ALG_SHA224 MBEDTLS_OID_DIGEST_ALG_SHA224
OID_DIGEST_ALG_SHA256
MBEDTLS_OID_DIGEST_ALG_SHA256
OID_DIGEST_ALG_SHA384 MBEDTLS_OID_DIGEST_ALG_SHA384
OID_DIGEST_ALG_SHA512 MBEDTLS_OID_DIGEST_ALG_SHA512
OID_DOMAIN_COMPONENT MBEDTLS_OID_DOMAIN_COMPONENT
OID_ECDSA_SHA1 MBEDTLS_OID_ECDSA_SHA1
OID_ECDSA_SHA224 MBEDTLS_OID_ECDSA_SHA224
OID_ECDSA_SHA256 MBEDTLS_OID_ECDSA_SHA256
OID_ECDSA_SHA384 MBEDTLS_OID_ECDSA_SHA384
OID_ECDSA_SHA512 MBEDTLS_OID_ECDSA_SHA512
OID_EC_ALG_ECDH MBEDTLS_OID_EC_ALG_ECDH
OID_EC_ALG_UNRESTRICTED MBEDTLS_OID_EC_ALG_UNRESTRICTED
OID_EC_BRAINPOOL_V1 MBEDTLS_OID_EC_BRAINPOOL_V1
OID_EC_GRP_BP256R1 MBEDTLS_OID_EC_GRP_BP256R1
OID_EC_GRP_BP384R1 MBEDTLS_OID_EC_GRP_BP384R1
OID_EC_GRP_BP512R1 MBEDTLS_OID_EC_GRP_BP512R1
OID_EC_GRP_SECP192K1 MBEDTLS_OID_EC_GRP_SECP192K1
OID_EC_GRP_SECP192R1 MBEDTLS_OID_EC_GRP_SECP192R1
OID_EC_GRP_SECP224K1 MBEDTLS_OID_EC_GRP_SECP224K1
OID_EC_GRP_SECP224R1 MBEDTLS_OID_EC_GRP_SECP224R1
OID_EC_GRP_SECP256K1 MBEDTLS_OID_EC_GRP_SECP256K1
OID_EC_GRP_SECP256R1 MBEDTLS_OID_EC_GRP_SECP256R1
OID_EC_GRP_SECP384R1
MBEDTLS_OID_EC_GRP_SECP384R1
OID_EC_GRP_SECP521R1 MBEDTLS_OID_EC_GRP_SECP521R1
OID_EMAIL_PROTECTION MBEDTLS_OID_EMAIL_PROTECTION
OID_EXTENDED_KEY_USAGE MBEDTLS_OID_EXTENDED_KEY_USAGE
OID_FRESHEST_CRL MBEDTLS_OID_FRESHEST_CRL
OID_GOV MBEDTLS_OID_GOV
OID_HMAC_SHA1 MBEDTLS_OID_HMAC_SHA1
OID_ID_CE MBEDTLS_OID_ID_CE
OID_INIHIBIT_ANYPOLICY MBEDTLS_OID_INIHIBIT_ANYPOLICY
OID_ISO_CCITT_DS MBEDTLS_OID_ISO_CCITT_DS
OID_ISO_IDENTIFIED_ORG MBEDTLS_OID_ISO_IDENTIFIED_ORG
OID_ISO_ITU_COUNTRY MBEDTLS_OID_ISO_ITU_COUNTRY

OID_ISO_ITU_US_ORG MBEDTLS_OID_ISO_ITU_US_ORG
OID_ISO_MEMBER_BODIES MBEDTLS_OID_ISO_MEMBER_BODIES
OID_ISSUER_ALT_NAME MBEDTLS_OID_ISSUER_ALT_NAME
OID_KEY_USAGE MBEDTLS_OID_KEY_USAGE
OID_KP MBEDTLS_OID_KP
OID_MGF1 MBEDTLS_OID_MGF1
OID_NAME_CONSTRAINTS MBEDTLS_OID_NAME_CONSTRAINTS
OID_NETSCAPE MBEDTLS_OID_NETSCAPE
OID_NS_BASE_URL MBEDTLS_OID_NS_BASE_URL
OID_NS_CA_POLICY_URL MBEDTLS_OID_NS_CA_POLICY_URL
OID_NS_CA_REVOCATION_URL MBEDTLS_OID_NS_CA_REVOCATION_URL
OID_NS_CERT
MBEDTLS_OID_NS_CERT
OID_NS_CERT_SEQUENCE MBEDTLS_OID_NS_CERT_SEQUENCE
OID_NS_CERT_TYPE MBEDTLS_OID_NS_CERT_TYPE
OID_NS_COMMENT MBEDTLS_OID_NS_COMMENT
OID_NS_DATA_TYPE MBEDTLS_OID_NS_DATA_TYPE
OID_NS_RENEWAL_URL MBEDTLS_OID_NS_RENEWAL_URL
OID_NS_REVOCATION_URL MBEDTLS_OID_NS_REVOCATION_URL
OID_NS_SSL_SERVER_NAME MBEDTLS_OID_NS_SSL_SERVER_NAME
OID_OCSP_SIGNING MBEDTLS_OID_OCSP_SIGNING
OID_OIW_SECSIG MBEDTLS_OID_OIW_SECSIG
OID_OIW_SECSIG_ALG MBEDTLS_OID_OIW_SECSIG_ALG
OID_OIW_SECSIG_SHA1 MBEDTLS_OID_OIW_SECSIG_SHA1
OID_ORGANIZATION MBEDTLS_OID_ORGANIZATION
OID_ORG_ANSI_X9_62 MBEDTLS_OID_ORG_ANSI_X9_62
OID_ORG_CERTICOM MBEDTLS_OID_ORG_CERTICOM
OID_ORG_DOD MBEDTLS_OID_ORG_DOD
OID_ORG_GOV MBEDTLS_OID_ORG_GOV
OID_ORG_NETSCAPE MBEDTLS_OID_ORG_NETSCAPE
OID_ORG_OIW MBEDTLS_OID_ORG_OIW
OID_ORG_RSA_DATA_SECURITY MBEDTLS_OID_ORG_RSA_DATA_SECURITY
OID_ORG_TELETRUST MBEDTLS_OID_ORG_TELETRUST
OID_PKCS MBEDTLS_OID_PKCS
OID_PKCS1 MBEDTLS_OID_PKCS1
OID_PKCS12 MBEDTLS_OID_PKCS12
OID_PKCS12_PBE MBEDTLS_OID_PKCS12_PBE
OID_PKCS12_PBE_SHA1_DES2_EDE_CBC
MBEDTLS_OID_PKCS12_PBE_SHA1_DES2_EDE_CBC
OID_PKCS12_PBE_SHA1_DES3_EDE_CBC MBEDTLS_OID_PKCS12_PBE_SHA1_DES3_EDE_CBC
OID_PKCS12_PBE_SHA1_RC2_128_CBC MBEDTLS_OID_PKCS12_PBE_SHA1_RC2_128_CBC
OID_PKCS12_PBE_SHA1_RC2_40_CBC MBEDTLS_OID_PKCS12_PBE_SHA1_RC2_40_CBC
OID_PKCS12_PBE_SHA1_RC4_128 MBEDTLS_OID_PKCS12_PBE_SHA1_RC4_128
OID_PKCS12_PBE_SHA1_RC4_40 MBEDTLS_OID_PKCS12_PBE_SHA1_RC4_40
OID_PKCS1_MD2 MBEDTLS_OID_PKCS1_MD2
OID_PKCS1_MD4 MBEDTLS_OID_PKCS1_MD4
OID_PKCS1_MD5 MBEDTLS_OID_PKCS1_MD5
OID_PKCS1_RSA MBEDTLS_OID_PKCS1_RSA

OID_PKCS1_SHA1 MBEDTLS_OID_PKCS1_SHA1
OID_PKCS1_SHA224 MBEDTLS_OID_PKCS1_SHA224
OID_PKCS1_SHA256 MBEDTLS_OID_PKCS1_SHA256
OID_PKCS1_SHA384 MBEDTLS_OID_PKCS1_SHA384
OID_PKCS1_SHA512 MBEDTLS_OID_PKCS1_SHA512
OID_PKCS5 MBEDTLS_OID_PKCS5
OID_PKCS5_PBES2 MBEDTLS_OID_PKCS5_PBES2
OID_PKCS5_PBE_MD2_DES_CBC MBEDTLS_OID_PKCS5_PBE_MD2_DES_CBC
OID_PKCS5_PBE_MD2_RC2_CBC MBEDTLS_OID_PKCS5_PBE_MD2_RC2_CBC
OID_PKCS5_PBE_MD5_DES_CBC MBEDTLS_OID_PKCS5_PBE_MD5_DES_CBC
OID_PKCS5_PBE_MD5_RC2_CBC
MBEDTLS_OID_PKCS5_PBE_MD5_RC2_CBC
OID_PKCS5_PBE_SHA1_DES_CBC MBEDTLS_OID_PKCS5_PBE_SHA1_DES_CBC
OID_PKCS5_PBE_SHA1_RC2_CBC MBEDTLS_OID_PKCS5_PBE_SHA1_RC2_CBC
OID_PKCS5_PBKDF2 MBEDTLS_OID_PKCS5_PBKDF2
OID_PKCS5_PBMAC1 MBEDTLS_OID_PKCS5_PBMAC1
OID_PKCS9 MBEDTLS_OID_PKCS9
OID_PKCS9_CSR_EXT_REQ MBEDTLS_OID_PKCS9_CSR_EXT_REQ
OID_PKCS9_EMAIL MBEDTLS_OID_PKCS9_EMAIL
OID_PKIX MBEDTLS_OID_PKIX
OID_POLICY_CONSTRAINTS MBEDTLS_OID_POLICY_CONSTRAINTS
OID_POLICY_MAPPINGS MBEDTLS_OID_POLICY_MAPPINGS
OID_PRIVATE_KEY_USAGE_PERIOD MBEDTLS_OID_PRIVATE_KEY_USAGE_PERIOD
OID_RSASSA_PSS MBEDTLS_OID_RSASSA_PSS
OID_RSA_COMPANY MBEDTLS_OID_RSA_COMPANY
OID_RSA_SHA_OBS MBEDTLS_OID_RSA_SHA_OBS
OID_SERVER_AUTH MBEDTLS_OID_SERVER_AUTH
OID_SIZE MBEDTLS_OID_SIZE
OID_SUBJECT_ALT_NAME MBEDTLS_OID_SUBJECT_ALT_NAME
OID_SUBJECT_DIRECTORY_ATTRS MBEDTLS_OID_SUBJECT_DIRECTORY_ATTRS
OID_SUBJECT_KEY_IDENTIFIER MBEDTLS_OID_SUBJECT_KEY_IDENTIFIER
OID_TELETRUST MBEDTLS_OID_TELETRUST
OID_TIME_STAMPING
MBEDTLS_OID_TIME_STAMPING
PADLOCK_ACE MBEDTLS_PADLOCK_ACE
PADLOCK_ALIGN16 MBEDTLS_PADLOCK_ALIGN16
PADLOCK_PHE MBEDTLS_PADLOCK_PHE
PADLOCK_PMM MBEDTLS_PADLOCK_PMM
PADLOCK_RNG MBEDTLS_PADLOCK_RNG
PKCS12_DERIVE_IV MBEDTLS_PKCS12_DERIVE_IV
PKCS12_DERIVE_KEY MBEDTLS_PKCS12_DERIVE_KEY
PKCS12_DERIVE_MAC_KEY MBEDTLS_PKCS12_DERIVE_MAC_KEY
PKCS12_PBE_DECRYPT MBEDTLS_PKCS12_PBE_DECRYPT
PKCS12_PBE_ENCRYPT MBEDTLS_PKCS12_PBE_ENCRYPT
PKCS5_DECRYPT MBEDTLS_PKCS5_DECRYPT
PKCS5_ENCRYPT MBEDTLS_PKCS5_ENCRYPT
POLARSSL_AESNI_AES MBEDTLS_AESNI_AES
POLARSSL_AESNI_C MBEDTLS_AESNI_C

POLARSSL_AESNI_CLMUL MBEDTLS_AESNI_CLMUL
POLARSSL_AESNI_H MBEDTLS_AESNI_H
POLARSSL_AES_ALT MBEDTLS_AES_ALT
POLARSSL_AES_C MBEDTLS_AES_C
POLARSSL_AES_H MBEDTLS_AES_H
POLARSSL_AES_ROM_TABLES MBEDTLS_AES_ROM_TABLES
POLARSSL_ARC4_ALT MBEDTLS_ARC4_ALT
POLARSSL_ARC4_C MBEDTLS_ARC4_C
POLARSSL_ARC4_H MBEDTLS_ARC4_H
POLARSSL_ASN1_H MBEDTLS_ASN1_H
POLARSSL_ASN1_PARSE_C MBEDTLS_ASN1_PARSE_C
POLARSSL_ASN1_WRITE_C
MBEDTLS_ASN1_WRITE_C
POLARSSL_ASN1_WRITE_H MBEDTLS_ASN1_WRITE_H
POLARSSL_BASE64_C MBEDTLS_BASE64_C
POLARSSL_BASE64_H MBEDTLS_BASE64_H
POLARSSL_BIGNUM_C MBEDTLS_BIGNUM_C
POLARSSL_BIGNUM_H MBEDTLS_BIGNUM_H
POLARSSL_BLOWFISH_ALT MBEDTLS_BLOWFISH_ALT
POLARSSL_BLOWFISH_C MBEDTLS_BLOWFISH_C
POLARSSL_BLOWFISH_H MBEDTLS_BLOWFISH_H
POLARSSL_BN_MUL_H MBEDTLS_BN_MUL_H
POLARSSL_CAMELLIA_ALT MBEDTLS_CAMELLIA_ALT
POLARSSL_CAMELLIA_C MBEDTLS_CAMELLIA_C
POLARSSL_CAMELLIA_H MBEDTLS_CAMELLIA_H
POLARSSL_CAMELLIA_SMALL_MEMORY MBEDTLS_CAMELLIA_SMALL_MEMORY
POLARSSL_CCM_C MBEDTLS_CCM_C
POLARSSL_CCM_H MBEDTLS_CCM_H
POLARSSL_CERTS_C MBEDTLS_CERTS_C
POLARSSL_CERTS_H MBEDTLS_CERTS_H
POLARSSL_CHECK_CONFIG_H MBEDTLS_CHECK_CONFIG_H
POLARSSL_CIPHERSUITE_NODTLS MBEDTLS_CIPHERSUITE_NODTLS
POLARSSL_CIPHERSUITE_SHORT_TAG MBEDTLS_CIPHERSUITE_SHORT_TAG
POLARSSL_CIPHERSUITE_WEAK MBEDTLS_CIPHERSUITE_WEAK
POLARSSL_CIPHER_AES_128_CBC MBEDTLS_CIPHER_AES_128_CBC
POLARSSL_CIPHER_AES_128_CCM MBEDTLS_CIPHER_AES_128_CCM
POLARSSL_CIPHER_AES_128_CFB128
MBEDTLS_CIPHER_AES_128_CFB128
POLARSSL_CIPHER_AES_128_CTR MBEDTLS_CIPHER_AES_128_CTR
POLARSSL_CIPHER_AES_128_ECB MBEDTLS_CIPHER_AES_128_ECB
POLARSSL_CIPHER_AES_128_GCM MBEDTLS_CIPHER_AES_128_GCM
POLARSSL_CIPHER_AES_192_CBC MBEDTLS_CIPHER_AES_192_CBC
POLARSSL_CIPHER_AES_192_CCM MBEDTLS_CIPHER_AES_192_CCM
POLARSSL_CIPHER_AES_192_CFB128 MBEDTLS_CIPHER_AES_192_CFB128
POLARSSL_CIPHER_AES_192_CTR MBEDTLS_CIPHER_AES_192_CTR
POLARSSL_CIPHER_AES_192_ECB MBEDTLS_CIPHER_AES_192_ECB
POLARSSL_CIPHER_AES_192_GCM MBEDTLS_CIPHER_AES_192_GCM
POLARSSL_CIPHER_AES_256_CBC MBEDTLS_CIPHER_AES_256_CBC

POLARSSL_CIPHER_AES_256_CCM MBEDTLS_CIPHER_AES_256_CCM
POLARSSL_CIPHER_AES_256_CFB128 MBEDTLS_CIPHER_AES_256_CFB128
POLARSSL_CIPHER_AES_256_CTR MBEDTLS_CIPHER_AES_256_CTR
POLARSSL_CIPHER_AES_256_ECB MBEDTLS_CIPHER_AES_256_ECB
POLARSSL_CIPHER_AES_256_GCM MBEDTLS_CIPHER_AES_256_GCM
POLARSSL_CIPHER_ARC4_128 MBEDTLS_CIPHER_ARC4_128
POLARSSL_CIPHER_BLOWFISH_CBC MBEDTLS_CIPHER_BLOWFISH_CBC
POLARSSL_CIPHER_BLOWFISH_CFB64
MBEDTLS_CIPHER_BLOWFISH_CFB64
POLARSSL_CIPHER_BLOWFISH_CTR MBEDTLS_CIPHER_BLOWFISH_CTR
POLARSSL_CIPHER_BLOWFISH_ECB MBEDTLS_CIPHER_BLOWFISH_ECB
POLARSSL_CIPHER_C MBEDTLS_CIPHER_C
POLARSSL_CIPHER_CAMELLIA_128_CBC MBEDTLS_CIPHER_CAMELLIA_128_CBC
POLARSSL_CIPHER_CAMELLIA_128_CCM MBEDTLS_CIPHER_CAMELLIA_128_CCM
POLARSSL_CIPHER_CAMELLIA_128_CFB128 MBEDTLS_CIPHER_CAMELLIA_128_CFB128
POLARSSL_CIPHER_CAMELLIA_128_CTR MBEDTLS_CIPHER_CAMELLIA_128_CTR
POLARSSL_CIPHER_CAMELLIA_128_ECB MBEDTLS_CIPHER_CAMELLIA_128_ECB
POLARSSL_CIPHER_CAMELLIA_128_GCM MBEDTLS_CIPHER_CAMELLIA_128_GCM
POLARSSL_CIPHER_CAMELLIA_192_CBC MBEDTLS_CIPHER_CAMELLIA_192_CBC
POLARSSL_CIPHER_CAMELLIA_192_CCM MBEDTLS_CIPHER_CAMELLIA_192_CCM
POLARSSL_CIPHER_CAMELLIA_192_CFB128 MBEDTLS_CIPHER_CAMELLIA_192_CFB128
POLARSSL_CIPHER_CAMELLIA_192_CTR MBEDTLS_CIPHER_CAMELLIA_192_CTR
POLARSSL_CIPHER_CAMELLIA_192_ECB MBEDTLS_CIPHER_CAMELLIA_192_ECB
POLARSSL_CIPHER_CAMELLIA_192_GCM MBEDTLS_CIPHER_CAMELLIA_192_GCM
POLARSSL_CIPHER_CAMELLIA_256_CBC
MBEDTLS_CIPHER_CAMELLIA_256_CBC
POLARSSL_CIPHER_CAMELLIA_256_CCM MBEDTLS_CIPHER_CAMELLIA_256_CCM
POLARSSL_CIPHER_CAMELLIA_256_CFB128 MBEDTLS_CIPHER_CAMELLIA_256_CFB128
POLARSSL_CIPHER_CAMELLIA_256_CTR MBEDTLS_CIPHER_CAMELLIA_256_CTR
POLARSSL_CIPHER_CAMELLIA_256_ECB MBEDTLS_CIPHER_CAMELLIA_256_ECB
POLARSSL_CIPHER_CAMELLIA_256_GCM MBEDTLS_CIPHER_CAMELLIA_256_GCM
POLARSSL_CIPHER_DES_CBC MBEDTLS_CIPHER_DES_CBC
POLARSSL_CIPHER_DES_ECB MBEDTLS_CIPHER_DES_ECB
POLARSSL_CIPHER_DES_EDE3_CBC MBEDTLS_CIPHER_DES_EDE3_CBC
POLARSSL_CIPHER_DES_EDE3_ECB MBEDTLS_CIPHER_DES_EDE3_ECB
POLARSSL_CIPHER_DES_EDE_CBC MBEDTLS_CIPHER_DES_EDE_CBC
POLARSSL_CIPHER_DES_EDE_ECB MBEDTLS_CIPHER_DES_EDE_ECB
POLARSSL_CIPHER_H MBEDTLS_CIPHER_H
POLARSSL_CIPHER_ID_3DES MBEDTLS_CIPHER_ID_3DES
POLARSSL_CIPHER_ID_AES MBEDTLS_CIPHER_ID_AES
POLARSSL_CIPHER_ID_ARC4 MBEDTLS_CIPHER_ID_ARC4
POLARSSL_CIPHER_ID_BLOWFISH MBEDTLS_CIPHER_ID_BLOWFISH
POLARSSL_CIPHER_ID_CAMELLIA MBEDTLS_CIPHER_ID_CAMELLIA
POLARSSL_CIPHER_ID_DES
MBEDTLS_CIPHER_ID_DES
POLARSSL_CIPHER_ID_NONE MBEDTLS_CIPHER_ID_NONE
POLARSSL_CIPHER_ID_NULL MBEDTLS_CIPHER_ID_NULL
POLARSSL_CIPHER_MODE_AEAD MBEDTLS_CIPHER_MODE_AEAD

POLARSSL_CIPHER_MODE_CBC MBEDTLS_CIPHER_MODE_CBC
POLARSSL_CIPHER_MODE_CFB MBEDTLS_CIPHER_MODE_CFB
POLARSSL_CIPHER_MODE_CTR MBEDTLS_CIPHER_MODE_CTR
POLARSSL_CIPHER_MODE_STREAM MBEDTLS_CIPHER_MODE_STREAM
POLARSSL_CIPHER_MODE_WITH_PADDING MBEDTLS_CIPHER_MODE_WITH_PADDING
POLARSSL_CIPHER_NONE MBEDTLS_CIPHER_NONE
POLARSSL_CIPHER_NULL MBEDTLS_CIPHER_NULL
POLARSSL_CIPHER_NULL_CIPHER MBEDTLS_CIPHER_NULL_CIPHER
POLARSSL_CIPHER_PADDING_ONE_AND_ZEROS MBEDTLS_CIPHER_PADDING_ONE_AND_ZEROS
POLARSSL_CIPHER_PADDING_PKCS7 MBEDTLS_CIPHER_PADDING_PKCS7
POLARSSL_CIPHER_PADDING_ZEROS MBEDTLS_CIPHER_PADDING_ZEROS
POLARSSL_CIPHER_PADDING_ZEROS_AND_LEN MBEDTLS_CIPHER_PADDING_ZEROS_AND_LEN
POLARSSL_CIPHER_VARIABLE_IV_LEN MBEDTLS_CIPHER_VARIABLE_IV_LEN
POLARSSL_CIPHER_VARIABLE_KEY_LEN MBEDTLS_CIPHER_VARIABLE_KEY_LEN
POLARSSL_CIPHER_WRAP_H
MBEDTLS_CIPHER_WRAP_H
POLARSSL_CONFIG_FILE MBEDTLS_CONFIG_FILE
POLARSSL_CONFIG_H MBEDTLS_CONFIG_H
POLARSSL_CTR_DRBG_C MBEDTLS_CTR_DRBG_C
POLARSSL_CTR_DRBG_H MBEDTLS_CTR_DRBG_H
POLARSSL_DEBUG_C MBEDTLS_DEBUG_C
POLARSSL_DEBUG_DFL_MODE MBEDTLS_DEBUG_DFL_MODE
POLARSSL_DEBUG_H MBEDTLS_DEBUG_H
POLARSSL_DEBUG_LOG_FULL MBEDTLS_DEBUG_LOG_FULL
POLARSSL_DEBUG_LOG_RAW MBEDTLS_DEBUG_LOG_RAW
POLARSSL_DECRYPT MBEDTLS_DECRYPT
POLARSSL_DEPRECATED_REMOVED MBEDTLS_DEPRECATED_REMOVED
POLARSSL_DEPRECATED_WARNING MBEDTLS_DEPRECATED_WARNING
POLARSSL_DES_ALT MBEDTLS_DES_ALT
POLARSSL_DES_C MBEDTLS_DES_C
POLARSSL_DES_H MBEDTLS_DES_H
POLARSSL_DHM_C MBEDTLS_DHM_C
POLARSSL_DHM_H MBEDTLS_DHM_H
POLARSSL_DHM_RFC2409_MODP_1024_G MBEDTLS_DHM_RFC2409_MODP_1024_G
POLARSSL_DHM_RFC2409_MODP_1024_P MBEDTLS_DHM_RFC2409_MODP_1024_P
POLARSSL_DHM_RFC3526_MODP_2048_G MBEDTLS_DHM_RFC3526_MODP_2048_G
POLARSSL_DHM_RFC3526_MODP_2048_P MBEDTLS_DHM_RFC3526_MODP_2048_P
POLARSSL_DHM_RFC3526_MODP_3072_G MBEDTLS_DHM_RFC3526_MODP_3072_G
POLARSSL_DHM_RFC3526_MODP_3072_P
MBEDTLS_DHM_RFC3526_MODP_3072_P
POLARSSL_DHM_RFC5114_MODP_1024_G MBEDTLS_DHM_RFC5114_MODP_1024_G
POLARSSL_DHM_RFC5114_MODP_1024_P MBEDTLS_DHM_RFC5114_MODP_1024_P
POLARSSL_DHM_RFC5114_MODP_2048_G MBEDTLS_DHM_RFC5114_MODP_2048_G
POLARSSL_DHM_RFC5114_MODP_2048_P MBEDTLS_DHM_RFC5114_MODP_2048_P
POLARSSL_ECDH_C MBEDTLS_ECDH_C
POLARSSL_ECDH_H MBEDTLS_ECDH_H
POLARSSL_ECDH_OURS MBEDTLS_ECDH_OURS
POLARSSL_ECDH_THEIRS MBEDTLS_ECDH_THEIRS

POLARSSL_ECDSA_C MBEDTLS_ECDSA_C
POLARSSL_ECDSA_DETERMINISTIC MBEDTLS_ECDSA_DETERMINISTIC
POLARSSL_ECDSA_H MBEDTLS_ECDSA_H
POLARSSL_ECP_C MBEDTLS_ECP_C
POLARSSL_ECP_DP_BP256R1 MBEDTLS_ECP_DP_BP256R1
POLARSSL_ECP_DP_BP256R1_ENABLED MBEDTLS_ECP_DP_BP256R1_ENABLED
POLARSSL_ECP_DP_BP384R1 MBEDTLS_ECP_DP_BP384R1
POLARSSL_ECP_DP_BP384R1_ENABLED MBEDTLS_ECP_DP_BP384R1_ENABLED
POLARSSL_ECP_DP_BP512R1 MBEDTLS_ECP_DP_BP512R1
POLARSSL_ECP_DP_BP512R1_ENABLED MBEDTLS_ECP_DP_BP512R1_ENABLED
POLARSSL_ECP_DP_M255 MBEDTLS_ECP_DP_CURVE25519
POLARSSL_ECP_DP_M255_ENABLED
MBEDTLS_ECP_DP_CURVE25519_ENABLED
POLARSSL_ECP_DP_MAX MBEDTLS_ECP_DP_MAX
POLARSSL_ECP_DP_NONE MBEDTLS_ECP_DP_NONE
POLARSSL_ECP_DP_SECP192K1 MBEDTLS_ECP_DP_SECP192K1
POLARSSL_ECP_DP_SECP192K1_ENABLED MBEDTLS_ECP_DP_SECP192K1_ENABLED
POLARSSL_ECP_DP_SECP192R1 MBEDTLS_ECP_DP_SECP192R1
POLARSSL_ECP_DP_SECP192R1_ENABLED MBEDTLS_ECP_DP_SECP192R1_ENABLED
POLARSSL_ECP_DP_SECP224K1 MBEDTLS_ECP_DP_SECP224K1
POLARSSL_ECP_DP_SECP224K1_ENABLED MBEDTLS_ECP_DP_SECP224K1_ENABLED
POLARSSL_ECP_DP_SECP224R1 MBEDTLS_ECP_DP_SECP224R1
POLARSSL_ECP_DP_SECP224R1_ENABLED MBEDTLS_ECP_DP_SECP224R1_ENABLED
POLARSSL_ECP_DP_SECP256K1 MBEDTLS_ECP_DP_SECP256K1
POLARSSL_ECP_DP_SECP256K1_ENABLED MBEDTLS_ECP_DP_SECP256K1_ENABLED
POLARSSL_ECP_DP_SECP256R1 MBEDTLS_ECP_DP_SECP256R1
POLARSSL_ECP_DP_SECP256R1_ENABLED MBEDTLS_ECP_DP_SECP256R1_ENABLED
POLARSSL_ECP_DP_SECP384R1 MBEDTLS_ECP_DP_SECP384R1
POLARSSL_ECP_DP_SECP384R1_ENABLED MBEDTLS_ECP_DP_SECP384R1_ENABLED
POLARSSL_ECP_DP_SECP521R1 MBEDTLS_ECP_DP_SECP521R1
POLARSSL_ECP_DP_SECP521R1_ENABLED
MBEDTLS_ECP_DP_SECP521R1_ENABLED
POLARSSL_ECP_FIXED_POINT_OPTIM MBEDTLS_ECP_FIXED_POINT_OPTIM
POLARSSL_ECP_H MBEDTLS_ECP_H
POLARSSL_ECP_MAX_BITS MBEDTLS_ECP_MAX_BITS
POLARSSL_ECP_MAX_BYTES MBEDTLS_ECP_MAX_BYTES
POLARSSL_ECP_MAX_PT_LEN MBEDTLS_ECP_MAX_PT_LEN
POLARSSL_ECP_NIST_OPTIM MBEDTLS_ECP_NIST_OPTIM
POLARSSL_ECP_PF_COMPRESSED MBEDTLS_ECP_PF_COMPRESSED
POLARSSL_ECP_PF_UNCOMPRESSED MBEDTLS_ECP_PF_UNCOMPRESSED
POLARSSL_ECP_TLS_NAMED_CURVE MBEDTLS_ECP_TLS_NAMED_CURVE
POLARSSL_ECP_WINDOW_SIZE MBEDTLS_ECP_WINDOW_SIZE
POLARSSL_ENABLE_WEAK_CIPHERSUITES MBEDTLS_ENABLE_WEAK_CIPHERSUITES
POLARSSL_ENCRYPT MBEDTLS_ENCRYPT
POLARSSL_ENTROPY_C MBEDTLS_ENTROPY_C
POLARSSL_ENTROPY_FORCE_SHA256 MBEDTLS_ENTROPY_FORCE_SHA256
POLARSSL_ENTROPY_H MBEDTLS_ENTROPY_H
POLARSSL_ENTROPY_POLL_H MBEDTLS_ENTROPY_POLL_H

POLARSSL_ENTROPY_SHA256_ACCUMULATOR MBEDTLS_ENTROPY_SHA256_ACCUMULATOR
POLARSSL_ENTROPY_SHA512_ACCUMULATOR MBEDTLS_ENTROPY_SHA512_ACCUMULATOR
POLARSSL_ERROR_C
MBEDTLS_ERROR_C
POLARSSL_ERROR_H MBEDTLS_ERROR_H
POLARSSL_ERROR_STRERROR_BC MBEDTLS_ERROR_STRERROR_BC
POLARSSL_ERROR_STRERROR_DUMMY MBEDTLS_ERROR_STRERROR_DUMMY
POLARSSL_ERR_AES_INVALID_INPUT_LENGTH MBEDTLS_ERR_AES_INVALID_INPUT_LENGTH
POLARSSL_ERR_AES_INVALID_KEY_LENGTH MBEDTLS_ERR_AES_INVALID_KEY_LENGTH
POLARSSL_ERR_ASN1_BUF_TOO_SMALL MBEDTLS_ERR_ASN1_BUF_TOO_SMALL
POLARSSL_ERR_ASN1_INVALID_DATA MBEDTLS_ERR_ASN1_INVALID_DATA
POLARSSL_ERR_ASN1_INVALID_LENGTH MBEDTLS_ERR_ASN1_INVALID_LENGTH
POLARSSL_ERR_ASN1_LENGTH_MISMATCH MBEDTLS_ERR_ASN1_LENGTH_MISMATCH
POLARSSL_ERR_ASN1_MALLOC_FAILED MBEDTLS_ERR_ASN1_ALLOC_FAILED
POLARSSL_ERR_ASN1_OUT_OF_DATA MBEDTLS_ERR_ASN1_OUT_OF_DATA
POLARSSL_ERR_ASN1_UNEXPECTED_TAG MBEDTLS_ERR_ASN1_UNEXPECTED_TAG
POLARSSL_ERR_BASE64_BUFFER_TOO_SMALL MBEDTLS_ERR_BASE64_BUFFER_TOO_SMALL
POLARSSL_ERR_BASE64_INVALID_CHARACTER MBEDTLS_ERR_BASE64_INVALID_CHARACTER
POLARSSL_ERR_BLOWFISH_INVALID_INPUT_LENGTH
MBEDTLS_ERR_BLOWFISH_INVALID_INPUT_LENGTH
POLARSSL_ERR_BLOWFISH_INVALID_KEY_LENGTH
MBEDTLS_ERR_BLOWFISH_INVALID_KEY_LENGTH
POLARSSL_ERR_CAMELLIA_INVALID_INPUT_LENGTH
MBEDTLS_ERR_CAMELLIA_INVALID_INPUT_LENGTH
POLARSSL_ERR_CAMELLIA_INVALID_KEY_LENGTH
MBEDTLS_ERR_CAMELLIA_INVALID_KEY_LENGTH
POLARSSL_ERR_CCM_AUTH_FAILED MBEDTLS_ERR_CCM_AUTH_FAILED
POLARSSL_ERR_CCM_BAD_INPUT MBEDTLS_ERR_CCM_BAD_INPUT
POLARSSL_ERR_CIPHER_ALLOC_FAILED MBEDTLS_ERR_CIPHER_ALLOC_FAILED
POLARSSL_ERR_CIPHER_AUTH_FAILED MBEDTLS_ERR_CIPHER_AUTH_FAILED
POLARSSL_ERR_CIPHER_BAD_INPUT_DATA MBEDTLS_ERR_CIPHER_BAD_INPUT_DATA
POLARSSL_ERR_CIPHER_FEATURE_UNAVAILABLE
MBEDTLS_ERR_CIPHER_FEATURE_UNAVAILABLE
POLARSSL_ERR_CIPHER_FULL_BLOCK_EXPECTED
MBEDTLS_ERR_CIPHER_FULL_BLOCK_EXPECTED
POLARSSL_ERR_CIPHER_INVALID_PADDING MBEDTLS_ERR_CIPHER_INVALID_PADDING
POLARSSL_ERR_CTR_DRBG_ENTROPY_SOURCE_FAILED
MBEDTLS_ERR_CTR_DRBG_ENTROPY_SOURCE_FAILED
POLARSSL_ERR_CTR_DRBG_FILE_IO_ERROR MBEDTLS_ERR_CTR_DRBG_FILE_IO_ERROR
POLARSSL_ERR_CTR_DRBG_INPUT_TOO_BIG MBEDTLS_ERR_CTR_DRBG_INPUT_TOO_BIG
POLARSSL_ERR_CTR_DRBG_REQUEST_TOO_BIG
MBEDTLS_ERR_CTR_DRBG_REQUEST_TOO_BIG
POLARSSL_ERR_DES_INVALID_INPUT_LENGTH MBEDTLS_ERR_DES_INVALID_INPUT_LENGTH
POLARSSL_ERR_DHM_BAD_INPUT_DATA MBEDTLS_ERR_DHM_BAD_INPUT_DATA
POLARSSL_ERR_DHM_CALC_SECRET_FAILED MBEDTLS_ERR_DHM_CALC_SECRET_FAILED
POLARSSL_ERR_DHM_FILE_IO_ERROR MBEDTLS_ERR_DHM_FILE_IO_ERROR
POLARSSL_ERR_DHM_INVALID_FORMAT MBEDTLS_ERR_DHM_INVALID_FORMAT
POLARSSL_ERR_DHM_MAKE_PARAMS_FAILED MBEDTLS_ERR_DHM_MAKE_PARAMS_FAILED

POLARSSL_ERR_DHM_MAKE_PUBLIC_FAILED MBEDTLS_ERR_DHM_MAKE_PUBLIC_FAILED
POLARSSL_ERR_DHM_MALLOC_FAILED MBEDTLS_ERR_DHM_ALLOC_FAILED
POLARSSL_ERR_DHM_READ_PARAMS_FAILED MBEDTLS_ERR_DHM_READ_PARAMS_FAILED
POLARSSL_ERR_DHM_READ_PUBLIC_FAILED MBEDTLS_ERR_DHM_READ_PUBLIC_FAILED
POLARSSL_ERR_ECP_BAD_INPUT_DATA MBEDTLS_ERR_ECP_BAD_INPUT_DATA
POLARSSL_ERR_ECP_BUFFER_TOO_SMALL MBEDTLS_ERR_ECP_BUFFER_TOO_SMALL
POLARSSL_ERR_ECP_FEATURE_UNAVAILABLE MBEDTLS_ERR_ECP_FEATURE_UNAVAILABLE
POLARSSL_ERR_ECP_INVALID_KEY MBEDTLS_ERR_ECP_INVALID_KEY
POLARSSL_ERR_ECP_MALLOC_FAILED
MBEDTLS_ERR_ECP_ALLOC_FAILED
POLARSSL_ERR_ECP_RANDOM_FAILED MBEDTLS_ERR_ECP_RANDOM_FAILED
POLARSSL_ERR_ECP_SIG_LEN_MISMATCH MBEDTLS_ERR_ECP_SIG_LEN_MISMATCH
POLARSSL_ERR_ECP_VERIFY_FAILED MBEDTLS_ERR_ECP_VERIFY_FAILED
POLARSSL_ERR_ENTROPY_FILE_IO_ERROR MBEDTLS_ERR_ENTROPY_FILE_IO_ERROR
POLARSSL_ERR_ENTROPY_MAX_SOURCES MBEDTLS_ERR_ENTROPY_MAX_SOURCES
POLARSSL_ERR_ENTROPY_NO_SOURCES_DEFINED
MBEDTLS_ERR_ENTROPY_NO_SOURCES_DEFINED
POLARSSL_ERR_ENTROPY_SOURCE_FAILED MBEDTLS_ERR_ENTROPY_SOURCE_FAILED
POLARSSL_ERR_GCM_AUTH_FAILED MBEDTLS_ERR_GCM_AUTH_FAILED
POLARSSL_ERR_GCM_BAD_INPUT MBEDTLS_ERR_GCM_BAD_INPUT
POLARSSL_ERR_HMAC_DRBG_ENTROPY_SOURCE_FAILED
MBEDTLS_ERR_HMAC_DRBG_ENTROPY_SOURCE_FAILED
POLARSSL_ERR_HMAC_DRBG_FILE_IO_ERROR MBEDTLS_ERR_HMAC_DRBG_FILE_IO_ERROR
POLARSSL_ERR_HMAC_DRBG_INPUT_TOO_BIG MBEDTLS_ERR_HMAC_DRBG_INPUT_TOO_BIG
POLARSSL_ERR_HMAC_DRBG_REQUEST_TOO_BIG
MBEDTLS_ERR_HMAC_DRBG_REQUEST_TOO_BIG
POLARSSL_ERR_MD2_FILE_IO_ERROR
MBEDTLS_ERR_MD2_FILE_IO_ERROR
POLARSSL_ERR_MD4_FILE_IO_ERROR MBEDTLS_ERR_MD4_FILE_IO_ERROR
POLARSSL_ERR_MD5_FILE_IO_ERROR MBEDTLS_ERR_MD5_FILE_IO_ERROR
POLARSSL_ERR_MD_ALLOC_FAILED MBEDTLS_ERR_MD_ALLOC_FAILED
POLARSSL_ERR_MD_BAD_INPUT_DATA MBEDTLS_ERR_MD_BAD_INPUT_DATA
POLARSSL_ERR_MD_FEATURE_UNAVAILABLE MBEDTLS_ERR_MD_FEATURE_UNAVAILABLE
POLARSSL_ERR_MD_FILE_IO_ERROR MBEDTLS_ERR_MD_FILE_IO_ERROR
POLARSSL_ERR_MPI_BAD_INPUT_DATA MBEDTLS_ERR_MPI_BAD_INPUT_DATA
POLARSSL_ERR_MPI_BUFFER_TOO_SMALL MBEDTLS_ERR_MPI_BUFFER_TOO_SMALL
POLARSSL_ERR_MPI_DIVISION_BY_ZERO MBEDTLS_ERR_MPI_DIVISION_BY_ZERO
POLARSSL_ERR_MPI_FILE_IO_ERROR MBEDTLS_ERR_MPI_FILE_IO_ERROR
POLARSSL_ERR_MPI_INVALID_CHARACTER MBEDTLS_ERR_MPI_INVALID_CHARACTER
POLARSSL_ERR_MPI_MALLOC_FAILED MBEDTLS_ERR_MPI_ALLOC_FAILED
POLARSSL_ERR_MPI_NEGATIVE_VALUE MBEDTLS_ERR_MPI_NEGATIVE_VALUE
POLARSSL_ERR_MPI_NOT_ACCEPTABLE MBEDTLS_ERR_MPI_NOT_ACCEPTABLE
POLARSSL_ERR_NET_ACCEPT_FAILED MBEDTLS_ERR_NET_ACCEPT_FAILED
POLARSSL_ERR_NET_BIND_FAILED
MBEDTLS_ERR_NET_BIND_FAILED
POLARSSL_ERR_NET_CONNECT_FAILED MBEDTLS_ERR_NET_CONNECT_FAILED
POLARSSL_ERR_NET_CONN_RESET MBEDTLS_ERR_NET_CONN_RESET
POLARSSL_ERR_NET_LISTEN_FAILED MBEDTLS_ERR_NET_LISTEN_FAILED

POLARSSL_ERR_NET_RECV_FAILED MBEDTLS_ERR_NET_RECV_FAILED
POLARSSL_ERR_NET_SEND_FAILED MBEDTLS_ERR_NET_SEND_FAILED
POLARSSL_ERR_NET_SOCKET_FAILED MBEDTLS_ERR_NET_SOCKET_FAILED
POLARSSL_ERR_NET_TIMEOUT MBEDTLS_ERR_SSL_TIMEOUT
POLARSSL_ERR_NET_UNKNOWN_HOST MBEDTLS_ERR_NET_UNKNOWN_HOST
POLARSSL_ERR_NET_WANT_READ MBEDTLS_ERR_SSL_WANT_READ
POLARSSL_ERR_NET_WANT_WRITE MBEDTLS_ERR_SSL_WANT_WRITE
POLARSSL_ERR_OID_BUF_TOO_SMALL MBEDTLS_ERR_OID_BUF_TOO_SMALL
POLARSSL_ERR_OID_NOT_FOUND MBEDTLS_ERR_OID_NOT_FOUND
POLARSSL_ERR_PADLOCK_DATA_MISALIGNED MBEDTLS_ERR_PADLOCK_DATA_MISALIGNED
POLARSSL_ERR_PBKDF2_BAD_INPUT_DATA MBEDTLS_ERR_PBKDF2_BAD_INPUT_DATA
POLARSSL_ERR_PEM_BAD_INPUT_DATA MBEDTLS_ERR_PEM_BAD_INPUT_DATA
POLARSSL_ERR_PEM_FEATURE_UNAVAILABLE MBEDTLS_ERR_PEM_FEATURE_UNAVAILABLE
POLARSSL_ERR_PEM_INVALID_DATA
MBEDTLS_ERR_PEM_INVALID_DATA
POLARSSL_ERR_PEM_INVALID_ENC_IV MBEDTLS_ERR_PEM_INVALID_ENC_IV
POLARSSL_ERR_PEM_MALLOC_FAILED MBEDTLS_ERR_PEM_ALLOC_FAILED
POLARSSL_ERR_PEM_NO_HEADER_FOOTER_PRESENT
MBEDTLS_ERR_PEM_NO_HEADER_FOOTER_PRESENT
POLARSSL_ERR_PEM_PASSWORD_MISMATCH MBEDTLS_ERR_PEM_PASSWORD_MISMATCH
POLARSSL_ERR_PEM_PASSWORD_REQUIRED MBEDTLS_ERR_PEM_PASSWORD_REQUIRED
POLARSSL_ERR_PEM_UNKNOWN_ENC_ALG MBEDTLS_ERR_PEM_UNKNOWN_ENC_ALG
POLARSSL_ERR_PKCS12_BAD_INPUT_DATA MBEDTLS_ERR_PKCS12_BAD_INPUT_DATA
POLARSSL_ERR_PKCS12_FEATURE_UNAVAILABLE
MBEDTLS_ERR_PKCS12_FEATURE_UNAVAILABLE
POLARSSL_ERR_PKCS12_PASSWORD_MISMATCH MBEDTLS_ERR_PKCS12_PASSWORD_MISMATCH
POLARSSL_ERR_PKCS12_PBE_INVALID_FORMAT MBEDTLS_ERR_PKCS12_PBE_INVALID_FORMAT
POLARSSL_ERR_PKCS5_BAD_INPUT_DATA MBEDTLS_ERR_PKCS5_BAD_INPUT_DATA
POLARSSL_ERR_PKCS5_FEATURE_UNAVAILABLE
MBEDTLS_ERR_PKCS5_FEATURE_UNAVAILABLE
POLARSSL_ERR_PKCS5_INVALID_FORMAT MBEDTLS_ERR_PKCS5_INVALID_FORMAT
POLARSSL_ERR_PKCS5_PASSWORD_MISMATCH
MBEDTLS_ERR_PKCS5_PASSWORD_MISMATCH
POLARSSL_ERR_PK_BAD_INPUT_DATA MBEDTLS_ERR_PK_BAD_INPUT_DATA
POLARSSL_ERR_PK_FEATURE_UNAVAILABLE MBEDTLS_ERR_PK_FEATURE_UNAVAILABLE
POLARSSL_ERR_PK_FILE_IO_ERROR MBEDTLS_ERR_PK_FILE_IO_ERROR
POLARSSL_ERR_PK_INVALID_ALG MBEDTLS_ERR_PK_INVALID_ALG
POLARSSL_ERR_PK_INVALID_PUBKEY MBEDTLS_ERR_PK_INVALID_PUBKEY
POLARSSL_ERR_PK_KEY_INVALID_FORMAT MBEDTLS_ERR_PK_KEY_INVALID_FORMAT
POLARSSL_ERR_PK_KEY_INVALID_VERSION MBEDTLS_ERR_PK_KEY_INVALID_VERSION
POLARSSL_ERR_PK_MALLOC_FAILED MBEDTLS_ERR_PK_ALLOC_FAILED
POLARSSL_ERR_PK_PASSWORD_MISMATCH MBEDTLS_ERR_PK_PASSWORD_MISMATCH
POLARSSL_ERR_PK_PASSWORD_REQUIRED MBEDTLS_ERR_PK_PASSWORD_REQUIRED
POLARSSL_ERR_PK_SIG_LEN_MISMATCH MBEDTLS_ERR_PK_SIG_LEN_MISMATCH
POLARSSL_ERR_PK_TYPE_MISMATCH MBEDTLS_ERR_PK_TYPE_MISMATCH
POLARSSL_ERR_PK_UNKNOWN_NAMED_CURVE MBEDTLS_ERR_PK_UNKNOWN_NAMED_CURVE
POLARSSL_ERR_PK_UNKNOWN_PK_ALG MBEDTLS_ERR_PK_UNKNOWN_PK_ALG
POLARSSL_ERR_RIPEMD160_FILE_IO_ERROR MBEDTLS_ERR_RIPEMD160_FILE_IO_ERROR

POLARSSL_ERR_RSA_BAD_INPUT_DATA
MBEDTLS_ERR_RSA_BAD_INPUT_DATA
POLARSSL_ERR_RSA_INVALID_PADDING MBEDTLS_ERR_RSA_INVALID_PADDING
POLARSSL_ERR_RSA_KEY_CHECK_FAILED MBEDTLS_ERR_RSA_KEY_CHECK_FAILED
POLARSSL_ERR_RSA_KEY_GEN_FAILED MBEDTLS_ERR_RSA_KEY_GEN_FAILED
POLARSSL_ERR_RSA_OUTPUT_TOO_LARGE MBEDTLS_ERR_RSA_OUTPUT_TOO_LARGE
POLARSSL_ERR_RSA_PRIVATE_FAILED MBEDTLS_ERR_RSA_PRIVATE_FAILED
POLARSSL_ERR_RSA_PUBLIC_FAILED MBEDTLS_ERR_RSA_PUBLIC_FAILED
POLARSSL_ERR_RSA_RNG_FAILED MBEDTLS_ERR_RSA_RNG_FAILED
POLARSSL_ERR_RSA_VERIFY_FAILED MBEDTLS_ERR_RSA_VERIFY_FAILED
POLARSSL_ERR_SHA1_FILE_IO_ERROR MBEDTLS_ERR_SHA1_FILE_IO_ERROR
POLARSSL_ERR_SHA256_FILE_IO_ERROR MBEDTLS_ERR_SHA256_FILE_IO_ERROR
POLARSSL_ERR_SHA512_FILE_IO_ERROR MBEDTLS_ERR_SHA512_FILE_IO_ERROR
POLARSSL_ERR_SSL_BAD_HS_CERTIFICATE MBEDTLS_ERR_SSL_BAD_HS_CERTIFICATE
POLARSSL_ERR_SSL_BAD_HS_CERTIFICATE_REQUEST
MBEDTLS_ERR_SSL_BAD_HS_CERTIFICATE_REQUEST
POLARSSL_ERR_SSL_BAD_HS_CERTIFICATE_VERIFY
MBEDTLS_ERR_SSL_BAD_HS_CERTIFICATE_VERIFY
POLARSSL_ERR_SSL_BAD_HS_CHANGE_CIPHER_SPEC
MBEDTLS_ERR_SSL_BAD_HS_CHANGE_CIPHER_SPEC
POLARSSL_ERR_SSL_BAD_HS_CLIENT_HELLO MBEDTLS_ERR_SSL_BAD_HS_CLIENT_HELLO
POLARSSL_ERR_SSL_BAD_HS_CLIENT_KEY_EXCHANGE
MBEDTLS_ERR_SSL_BAD_HS_CLIENT_KEY_EXCHANGE
POLARSSL_ERR_SSL_BAD_HS_CLIENT_KEY_EXCHANGE_CS
MBEDTLS_ERR_SSL_BAD_HS_CLIENT_KEY_EXCHANGE_CS
POLARSSL_ERR_SSL_BAD_HS_CLIENT_KEY_EXCHANGE_RP
MBEDTLS_ERR_SSL_BAD_HS_CLIENT_KEY_EXCHANGE_RP
POLARSSL_ERR_SSL_BAD_HS_FINISHED MBEDTLS_ERR_SSL_BAD_HS_FINISHED
POLARSSL_ERR_SSL_BAD_HS_NEW_SESSION_TICKET
MBEDTLS_ERR_SSL_BAD_HS_NEW_SESSION_TICKET
POLARSSL_ERR_SSL_BAD_HS_PROTOCOL_VERSION
MBEDTLS_ERR_SSL_BAD_HS_PROTOCOL_VERSION
POLARSSL_ERR_SSL_BAD_HS_SERVER_HELLO MBEDTLS_ERR_SSL_BAD_HS_SERVER_HELLO
POLARSSL_ERR_SSL_BAD_HS_SERVER_HELLO_DONE
MBEDTLS_ERR_SSL_BAD_HS_SERVER_HELLO_DONE
POLARSSL_ERR_SSL_BAD_HS_SERVER_KEY_EXCHANGE
MBEDTLS_ERR_SSL_BAD_HS_SERVER_KEY_EXCHANGE
POLARSSL_ERR_SSL_BAD_INPUT_DATA MBEDTLS_ERR_SSL_BAD_INPUT_DATA
POLARSSL_ERR_SSL_BUFFER_TOO_SMALL
MBEDTLS_ERR_SSL_BUFFER_TOO_SMALL
POLARSSL_ERR_SSL_CA_CHAIN_REQUIRED MBEDTLS_ERR_SSL_CA_CHAIN_REQUIRED
POLARSSL_ERR_SSL_CERTIFICATE_REQUIRED MBEDTLS_ERR_SSL_CERTIFICATE_REQUIRED
POLARSSL_ERR_SSL_CERTIFICATE_TOO_LARGE MBEDTLS_ERR_SSL_CERTIFICATE_TOO_LARGE
POLARSSL_ERR_SSL_COMPRESSION_FAILED MBEDTLS_ERR_SSL_COMPRESSION_FAILED
POLARSSL_ERR_SSL_CONN_EOF MBEDTLS_ERR_SSL_CONN_EOF
POLARSSL_ERR_SSL_COUNTER_WRAPPING MBEDTLS_ERR_SSL_COUNTER_WRAPPING
POLARSSL_ERR_SSL_FATAL_ALERT_MESSAGE MBEDTLS_ERR_SSL_FATAL_ALERT_MESSAGE
POLARSSL_ERR_SSL_FEATURE_UNAVAILABLE MBEDTLS_ERR_SSL_FEATURE_UNAVAILABLE

POLARSSL_ERR_SSL_HELLO_VERIFY_REQUIRED MBEDTLS_ERR_SSL_HELLO_VERIFY_REQUIRED
POLARSSL_ERR_SSL_HW_ACCEL_FAILED MBEDTLS_ERR_SSL_HW_ACCEL_FAILED
POLARSSL_ERR_SSL_HW_ACCEL_FALLTHROUGH
MBEDTLS_ERR_SSL_HW_ACCEL_FALLTHROUGH
POLARSSL_ERR_SSL_INTERNAL_ERROR MBEDTLS_ERR_SSL_INTERNAL_ERROR
POLARSSL_ERR_SSL_INVALID_MAC MBEDTLS_ERR_SSL_INVALID_MAC
POLARSSL_ERR_SSL_INVALID_RECORD MBEDTLS_ERR_SSL_INVALID_RECORD
POLARSSL_ERR_SSL_MALLOC_FAILED
MBEDTLS_ERR_SSL_ALLOC_FAILED
POLARSSL_ERR_SSL_NO_CIPHER_CHOSEN MBEDTLS_ERR_SSL_NO_CIPHER_CHOSEN
POLARSSL_ERR_SSL_NO_CLIENT_CERTIFICATE MBEDTLS_ERR_SSL_NO_CLIENT_CERTIFICATE
POLARSSL_ERR_SSL_NO_RNG MBEDTLS_ERR_SSL_NO_RNG
POLARSSL_ERR_SSL_NO_USABLE_CIPHERSUITE MBEDTLS_ERR_SSL_NO_USABLE_CIPHERSUITE
POLARSSL_ERR_SSL_PEER_CLOSE_NOTIFY MBEDTLS_ERR_SSL_PEER_CLOSE_NOTIFY
POLARSSL_ERR_SSL_PEER_VERIFY_FAILED MBEDTLS_ERR_SSL_PEER_VERIFY_FAILED
POLARSSL_ERR_SSL_PK_TYPE_MISMATCH MBEDTLS_ERR_SSL_PK_TYPE_MISMATCH
POLARSSL_ERR_SSL_PRIVATE_KEY_REQUIRED MBEDTLS_ERR_SSL_PRIVATE_KEY_REQUIRED
POLARSSL_ERR_SSL_SESSION_TICKET_EXPIRED MBEDTLS_ERR_SSL_SESSION_TICKET_EXPIRED
POLARSSL_ERR_SSL_UNEXPECTED_MESSAGE MBEDTLS_ERR_SSL_UNEXPECTED_MESSAGE
POLARSSL_ERR_SSL_UNKNOWN_CIPHER MBEDTLS_ERR_SSL_UNKNOWN_CIPHER
POLARSSL_ERR_SSL_UNKNOWN_IDENTITY MBEDTLS_ERR_SSL_UNKNOWN_IDENTITY
POLARSSL_ERR_SSL_WAITING_SERVER_HELLO_RENEGO
MBEDTLS_ERR_SSL_WAITING_SERVER_HELLO_RENEGO
POLARSSL_ERR_THREADING_BAD_INPUT_DATA
MBEDTLS_ERR_THREADING_BAD_INPUT_DATA
POLARSSL_ERR_THREADING_FEATURE_UNAVAILABLE
MBEDTLS_ERR_THREADING_FEATURE_UNAVAILABLE
POLARSSL_ERR_THREADING_MUTEX_ERROR MBEDTLS_ERR_THREADING_MUTEX_ERROR
POLARSSL_ERR_X509_BAD_INPUT_DATA MBEDTLS_ERR_X509_BAD_INPUT_DATA
POLARSSL_ERR_X509_CERT_UNKNOWN_FORMAT
MBEDTLS_ERR_X509_CERT_UNKNOWN_FORMAT
POLARSSL_ERR_X509_CERT_VERIFY_FAILED MBEDTLS_ERR_X509_CERT_VERIFY_FAILED
POLARSSL_ERR_X509_FEATURE_UNAVAILABLE MBEDTLS_ERR_X509_FEATURE_UNAVAILABLE
POLARSSL_ERR_X509_FILE_IO_ERROR MBEDTLS_ERR_X509_FILE_IO_ERROR
POLARSSL_ERR_X509_INVALID_ALG MBEDTLS_ERR_X509_INVALID_ALG
POLARSSL_ERR_X509_INVALID_DATE MBEDTLS_ERR_X509_INVALID_DATE
POLARSSL_ERR_X509_INVALID_EXTENSIONS MBEDTLS_ERR_X509_INVALID_EXTENSIONS
POLARSSL_ERR_X509_INVALID_FORMAT MBEDTLS_ERR_X509_INVALID_FORMAT
POLARSSL_ERR_X509_INVALID_NAME MBEDTLS_ERR_X509_INVALID_NAME
POLARSSL_ERR_X509_INVALID_SERIAL MBEDTLS_ERR_X509_INVALID_SERIAL
POLARSSL_ERR_X509_INVALID_SIGNATURE MBEDTLS_ERR_X509_INVALID_SIGNATURE
POLARSSL_ERR_X509_INVALID_VERSION
MBEDTLS_ERR_X509_INVALID_VERSION
POLARSSL_ERR_X509_MALLOC_FAILED MBEDTLS_ERR_X509_ALLOC_FAILED
POLARSSL_ERR_X509_SIG_MISMATCH MBEDTLS_ERR_X509_SIG_MISMATCH
POLARSSL_ERR_X509_UNKNOWN_OID MBEDTLS_ERR_X509_UNKNOWN_OID
POLARSSL_ERR_X509_UNKNOWN_SIG_ALG MBEDTLS_ERR_X509_UNKNOWN_SIG_ALG
POLARSSL_ERR_X509_UNKNOWN_VERSION MBEDTLS_ERR_X509_UNKNOWN_VERSION

POLARSSL_ERR_XTEA_INVALID_INPUT_LENGTH MBEDTLS_ERR_XTEA_INVALID_INPUT_LENGTH
POLARSSL_FS_IO MBEDTLS_FS_IO
POLARSSL_GCM_C MBEDTLS_GCM_C
POLARSSL_GCM_H MBEDTLS_GCM_H
POLARSSL_GENPRIME MBEDTLS_GENPRIME
POLARSSL_HAVEGE_C MBEDTLS_HAVEGE_C
POLARSSL_HAVEGE_H MBEDTLS_HAVEGE_H
POLARSSL_HAVE_ASM MBEDTLS_HAVE_ASM
POLARSSL_HAVE_INT16 MBEDTLS_HAVE_INT16
POLARSSL_HAVE_INT32 MBEDTLS_HAVE_INT32
POLARSSL_HAVE_INT64 MBEDTLS_HAVE_INT64
POLARSSL_HAVE_INT8 MBEDTLS_HAVE_INT8
POLARSSL_HAVE_IPV6 MBEDTLS_HAVE_IPV6
POLARSSL_HAVE_LONGLONG MBEDTLS_HAVE_LONGLONG
POLARSSL_HAVE_SSE2 MBEDTLS_HAVE_SSE2
POLARSSL_HAVE_TIME
MBEDTLS_HAVE_TIME
POLARSSL_HAVE_UDBL MBEDTLS_HAVE_UDBL
POLARSSL_HAVE_X86 MBEDTLS_HAVE_X86
POLARSSL_HAVE_X86_64 MBEDTLS_HAVE_X86_64
POLARSSL_HMAC_DRBG_C MBEDTLS_HMAC_DRBG_C
POLARSSL_HMAC_DRBG_H MBEDTLS_HMAC_DRBG_H
POLARSSL_HMAC_DRBG_MAX_INPUT MBEDTLS_HMAC_DRBG_MAX_INPUT
POLARSSL_HMAC_DRBG_MAX_REQUEST MBEDTLS_HMAC_DRBG_MAX_REQUEST
POLARSSL_HMAC_DRBG_MAX_SEED_INPUT MBEDTLS_HMAC_DRBG_MAX_SEED_INPUT
POLARSSL_HMAC_DRBG_PR_OFF MBEDTLS_HMAC_DRBG_PR_OFF
POLARSSL_HMAC_DRBG_PR_ON MBEDTLS_HMAC_DRBG_PR_ON
POLARSSL_HMAC_DRBG_RESEED_INTERVAL MBEDTLS_HMAC_DRBG_RESEED_INTERVAL
POLARSSL_KEY_EXCHANGE_DHE_PSK MBEDTLS_KEY_EXCHANGE_DHE_PSK
POLARSSL_KEY_EXCHANGE_DHE_PSK_ENABLED
MBEDTLS_KEY_EXCHANGE_DHE_PSK_ENABLED
POLARSSL_KEY_EXCHANGE_DHE_RSA MBEDTLS_KEY_EXCHANGE_DHE_RSA
POLARSSL_KEY_EXCHANGE_DHE_RSA_ENABLED
MBEDTLS_KEY_EXCHANGE_DHE_RSA_ENABLED
POLARSSL_KEY_EXCHANGE_ECDHE_ECDSA MBEDTLS_KEY_EXCHANGE_ECDHE_ECDSA
POLARSSL_KEY_EXCHANGE_ECDHE_ECDSA_ENABLED
MBEDTLS_KEY_EXCHANGE_ECDHE_ECDSA_ENABLED
POLARSSL_KEY_EXCHANGE_ECDHE_PSK
MBEDTLS_KEY_EXCHANGE_ECDHE_PSK
POLARSSL_KEY_EXCHANGE_ECDHE_PSK_ENABLED
MBEDTLS_KEY_EXCHANGE_ECDHE_PSK_ENABLED
POLARSSL_KEY_EXCHANGE_ECDHE_RSA MBEDTLS_KEY_EXCHANGE_ECDHE_RSA
POLARSSL_KEY_EXCHANGE_ECDHE_RSA_ENABLED
MBEDTLS_KEY_EXCHANGE_ECDHE_RSA_ENABLED
POLARSSL_KEY_EXCHANGE_ECDH_ECDSA MBEDTLS_KEY_EXCHANGE_ECDH_ECDSA
POLARSSL_KEY_EXCHANGE_ECDH_ECDSA_ENABLED
MBEDTLS_KEY_EXCHANGE_ECDH_ECDSA_ENABLED
POLARSSL_KEY_EXCHANGE_ECDH_RSA MBEDTLS_KEY_EXCHANGE_ECDH_RSA

POLARSSL_KEY_EXCHANGE_ECDH_RSA_ENABLED
MBEDTLS_KEY_EXCHANGE_ECDH_RSA_ENABLED
POLARSSL_KEY_EXCHANGE_NONE MBEDTLS_KEY_EXCHANGE_NONE
POLARSSL_KEY_EXCHANGE_PSK MBEDTLS_KEY_EXCHANGE_PSK
POLARSSL_KEY_EXCHANGE_PSK_ENABLED MBEDTLS_KEY_EXCHANGE_PSK_ENABLED
POLARSSL_KEY_EXCHANGE_RSA MBEDTLS_KEY_EXCHANGE_RSA
POLARSSL_KEY_EXCHANGE_RSA_ENABLED MBEDTLS_KEY_EXCHANGE_RSA_ENABLED
POLARSSL_KEY_EXCHANGE_RSA_PSK MBEDTLS_KEY_EXCHANGE_RSA_PSK
POLARSSL_KEY_EXCHANGE_RSA_PSK_ENABLED
MBEDTLS_KEY_EXCHANGE_RSA_PSK_ENABLED
POLARSSL_KEY_EXCHANGE__SOME__ECDHE_ENABLED
MBEDTLS_KEY_EXCHANGE__SOME__ECDHE_ENABLED
POLARSSL_KEY_EXCHANGE__SOME__PSK_ENABLED
MBEDTLS_KEY_EXCHANGE__SOME__PSK_ENABLED
POLARSSL_KEY_EXCHANGE__WITH_CERT__ENABLED
MBEDTLS_KEY_EXCHANGE__WITH_CERT__ENABLED
POLARSSL_KEY_LENGTH_DES MBEDTLS_KEY_LENGTH_DES
POLARSSL_KEY_LENGTH_DES_EDE MBEDTLS_KEY_LENGTH_DES_EDE
POLARSSL_KEY_LENGTH_DES_EDE3 MBEDTLS_KEY_LENGTH_DES_EDE3
POLARSSL_KEY_LENGTH_NONE MBEDTLS_KEY_LENGTH_NONE
POLARSSL_MAX_BLOCK_LENGTH MBEDTLS_MAX_BLOCK_LENGTH
POLARSSL_MAX_IV_LENGTH MBEDTLS_MAX_IV_LENGTH
POLARSSL_MD2_ALT MBEDTLS_MD2_ALT
POLARSSL_MD2_C MBEDTLS_MD2_C
POLARSSL_MD2_H MBEDTLS_MD2_H
POLARSSL_MD4_ALT MBEDTLS_MD4_ALT
POLARSSL_MD4_C MBEDTLS_MD4_C
POLARSSL_MD4_H MBEDTLS_MD4_H
POLARSSL_MD5_ALT MBEDTLS_MD5_ALT
POLARSSL_MD5_C MBEDTLS_MD5_C
POLARSSL_MD5_H MBEDTLS_MD5_H
POLARSSL_MD_C MBEDTLS_MD_C
POLARSSL_MD_H MBEDTLS_MD_H
POLARSSL_MD_MAX_SIZE MBEDTLS_MD_MAX_SIZE
POLARSSL_MD_MD2 MBEDTLS_MD_MD2
POLARSSL_MD_MD4 MBEDTLS_MD_MD4
POLARSSL_MD_MD5 MBEDTLS_MD_MD5
POLARSSL_MD_NONE
MBEDTLS_MD_NONE
POLARSSL_MD_RIPEMD160 MBEDTLS_MD_RIPEMD160
POLARSSL_MD_SHA1 MBEDTLS_MD_SHA1
POLARSSL_MD_SHA224 MBEDTLS_MD_SHA224
POLARSSL_MD_SHA256 MBEDTLS_MD_SHA256
POLARSSL_MD_SHA384 MBEDTLS_MD_SHA384
POLARSSL_MD_SHA512 MBEDTLS_MD_SHA512
POLARSSL_MD_WRAP_H MBEDTLS_MD_WRAP_H
POLARSSL_MEMORY_ALIGN_MULTIPLE MBEDTLS_MEMORY_ALIGN_MULTIPLE
POLARSSL_MEMORY_BACKTRACE MBEDTLS_MEMORY_BACKTRACE

POLARSSL_MEMORY_BUFFER_ALLOC_C MBEDTLS_MEMORY_BUFFER_ALLOC_C
POLARSSL_MEMORY_BUFFER_ALLOC_H MBEDTLS_MEMORY_BUFFER_ALLOC_H
POLARSSL_MEMORY_C MBEDTLS_MEMORY_C
POLARSSL_MEMORY_DEBUG MBEDTLS_MEMORY_DEBUG
POLARSSL_MEMORY_H MBEDTLS_MEMORY_H
POLARSSL_MODE_CBC MBEDTLS_MODE_CBC
POLARSSL_MODE_CCM MBEDTLS_MODE_CCM
POLARSSL_MODE_CFB MBEDTLS_MODE_CFB
POLARSSL_MODE_CTR MBEDTLS_MODE_CTR
POLARSSL_MODE_ECB MBEDTLS_MODE_ECB
POLARSSL_MODE_GCM MBEDTLS_MODE_GCM
POLARSSL_MODE_NONE MBEDTLS_MODE_NONE
POLARSSL_MODE_OFB MBEDTLS_MODE_OFB
POLARSSL_MODE_STREAM MBEDTLS_MODE_STREAM
POLARSSL_MPI_MAX_BITS MBEDTLS_MPI_MAX_BITS
POLARSSL_MPI_MAX_BITS_SCALE100
MBEDTLS_MPI_MAX_BITS_SCALE100
POLARSSL_MPI_MAX_LIMBS MBEDTLS_MPI_MAX_LIMBS
POLARSSL_MPI_MAX_SIZE MBEDTLS_MPI_MAX_SIZE
POLARSSL_MPI_RW_BUFFER_SIZE MBEDTLS_MPI_RW_BUFFER_SIZE
POLARSSL_MPI_WINDOW_SIZE MBEDTLS_MPI_WINDOW_SIZE
POLARSSL_NET_C MBEDTLS_NET_C
POLARSSL_NET_H MBEDTLS_NET_H
POLARSSL_NET_LISTEN_BACKLOG MBEDTLS_NET_LISTEN_BACKLOG
POLARSSL_NO_DEFAULT_ENTROPY_SOURCES MBEDTLS_NO_DEFAULT_ENTROPY_SOURCES
POLARSSL_NO_PLATFORM_ENTROPY MBEDTLS_NO_PLATFORM_ENTROPY
POLARSSL_OID_C MBEDTLS_OID_C
POLARSSL_OID_H MBEDTLS_OID_H
POLARSSL_OPERATION_NONE MBEDTLS_OPERATION_NONE
POLARSSL_PADDING_NONE MBEDTLS_PADDING_NONE
POLARSSL_PADDING_ONE_AND_ZEROS MBEDTLS_PADDING_ONE_AND_ZEROS
POLARSSL_PADDING_PKCS7 MBEDTLS_PADDING_PKCS7
POLARSSL_PADDING_ZEROS MBEDTLS_PADDING_ZEROS
POLARSSL_PADDING_ZEROS_AND_LEN MBEDTLS_PADDING_ZEROS_AND_LEN
POLARSSL_PADLOCK_C MBEDTLS_PADLOCK_C
POLARSSL_PADLOCK_H MBEDTLS_PADLOCK_H
POLARSSL_PBKDF2_C MBEDTLS_PBKDF2_C
POLARSSL_PBKDF2_H MBEDTLS_PBKDF2_H
POLARSSL_PEM_H
MBEDTLS_PEM_H
POLARSSL_PEM_PARSE_C MBEDTLS_PEM_PARSE_C
POLARSSL_PEM_WRITE_C MBEDTLS_PEM_WRITE_C
POLARSSL_PKCS11_C MBEDTLS_PKCS11_C
POLARSSL_PKCS11_H MBEDTLS_PKCS11_H
POLARSSL_PKCS12_C MBEDTLS_PKCS12_C
POLARSSL_PKCS12_H MBEDTLS_PKCS12_H
POLARSSL_PKCS1_V15 MBEDTLS_PKCS1_V15
POLARSSL_PKCS1_V21 MBEDTLS_PKCS1_V21

POLARSSL_PKCS5_C MBEDTLS_PKCS5_C
POLARSSL_PKCS5_H MBEDTLS_PKCS5_H
POLARSSL_PK_C MBEDTLS_PK_C
POLARSSL_PK_DEBUG_ECP MBEDTLS_PK_DEBUG_ECP
POLARSSL_PK_DEBUG_MAX_ITEMS MBEDTLS_PK_DEBUG_MAX_ITEMS
POLARSSL_PK_DEBUG_MPI MBEDTLS_PK_DEBUG_MPI
POLARSSL_PK_DEBUG_NONE MBEDTLS_PK_DEBUG_NONE
POLARSSL_PK_ECDSA MBEDTLS_PK_ECDSA
POLARSSL_PK_ECKEY MBEDTLS_PK_ECKEY
POLARSSL_PK_ECKEY_DH MBEDTLS_PK_ECKEY_DH
POLARSSL_PK_H MBEDTLS_PK_H
POLARSSL_PK_NONE MBEDTLS_PK_NONE
POLARSSL_PK_PARSE_C MBEDTLS_PK_PARSE_C
POLARSSL_PK_PARSE_EC_EXTENDED MBEDTLS_PK_PARSE_EC_EXTENDED
POLARSSL_PK_RSA MBEDTLS_PK_RSA
POLARSSL_PK_RSASSA_PSS MBEDTLS_PK_RSASSA_PSS
POLARSSL_PK_RSA_ALT MBEDTLS_PK_RSA_ALT
POLARSSL_PK_WRAP_H
MBEDTLS_PK_WRAP_H
POLARSSL_PK_WRITE_C MBEDTLS_PK_WRITE_C
POLARSSL_PLATFORM_C MBEDTLS_PLATFORM_C
POLARSSL_PLATFORM_EXIT_ALT MBEDTLS_PLATFORM_EXIT_ALT
POLARSSL_PLATFORM_EXIT_MACRO MBEDTLS_PLATFORM_EXIT_MACRO
POLARSSL_PLATFORM_FPRINTF_ALT MBEDTLS_PLATFORM_FPRINTF_ALT
POLARSSL_PLATFORM_FPRINTF_MACRO MBEDTLS_PLATFORM_FPRINTF_MACRO
POLARSSL_PLATFORM_FREE_MACRO MBEDTLS_PLATFORM_FREE_MACRO
POLARSSL_PLATFORM_H MBEDTLS_PLATFORM_H
POLARSSL_PLATFORM_MALLOC_MACRO MBEDTLS_PLATFORM_ALLOC_MACRO
POLARSSL_PLATFORM_MEMORY MBEDTLS_PLATFORM_MEMORY
POLARSSL_PLATFORM_NO_STD_FUNCTIONS MBEDTLS_PLATFORM_NO_STD_FUNCTIONS
POLARSSL_PLATFORM_PRINTF_ALT MBEDTLS_PLATFORM_PRINTF_ALT
POLARSSL_PLATFORM_PRINTF_MACRO MBEDTLS_PLATFORM_PRINTF_MACRO
POLARSSL_PLATFORM_SNPRINTF_ALT MBEDTLS_PLATFORM_SNPRINTF_ALT
POLARSSL_PLATFORM_SNPRINTF_MACRO MBEDTLS_PLATFORM_SNPRINTF_MACRO
POLARSSL_PLATFORM_STD_EXIT MBEDTLS_PLATFORM_STD_EXIT
POLARSSL_PLATFORM_STD_FPRINTF MBEDTLS_PLATFORM_STD_FPRINTF
POLARSSL_PLATFORM_STD_FREE MBEDTLS_PLATFORM_STD_FREE
POLARSSL_PLATFORM_STD_MALLOC
MBEDTLS_PLATFORM_STD_CALLOC
POLARSSL_PLATFORM_STD_MEM_HDR MBEDTLS_PLATFORM_STD_MEM_HDR
POLARSSL_PLATFORM_STD_PRINTF MBEDTLS_PLATFORM_STD_PRINTF
POLARSSL_PLATFORM_STD_SNPRINTF MBEDTLS_PLATFORM_STD_SNPRINTF
POLARSSL_PREMASTER_SIZE MBEDTLS_PREMASTER_SIZE
POLARSSL_PSK_MAX_LEN MBEDTLS_PSK_MAX_LEN
POLARSSL_REMOVE_ARC4_CIPHERSUITES MBEDTLS_REMOVE_ARC4_CIPHERSUITES
POLARSSL_RIPEMD160_ALT MBEDTLS_RIPEMD160_ALT
POLARSSL_RIPEMD160_C MBEDTLS_RIPEMD160_C
POLARSSL_RIPEMD160_H MBEDTLS_RIPEMD160_H

POLARSSL_RSA_C MBEDTLS_RSA_C
POLARSSL_RSA_H MBEDTLS_RSA_H
POLARSSL_RSA_NO_CRT MBEDTLS_RSA_NO_CRT
POLARSSL_SELF_TEST MBEDTLS_SELF_TEST
POLARSSL_SHA1_ALT MBEDTLS_SHA1_ALT
POLARSSL_SHA1_C MBEDTLS_SHA1_C
POLARSSL_SHA1_H MBEDTLS_SHA1_H
POLARSSL_SHA256_ALT MBEDTLS_SHA256_ALT
POLARSSL_SHA256_C MBEDTLS_SHA256_C
POLARSSL_SHA256_H MBEDTLS_SHA256_H
POLARSSL_SHA512_ALT MBEDTLS_SHA512_ALT
POLARSSL_SHA512_C MBEDTLS_SHA512_C
POLARSSL_SHA512_H MBEDTLS_SHA512_H
POLARSSL_SSL_AEAD_RANDOM_IV
MBEDTLS_SSL_AEAD_RANDOM_IV
POLARSSL_SSL_ALERT_MESSAGES MBEDTLS_SSL_ALERT_MESSAGES
POLARSSL_SSL_ALPN MBEDTLS_SSL_ALPN
POLARSSL_SSL_CACHE_C MBEDTLS_SSL_CACHE_C
POLARSSL_SSL_CACHE_H MBEDTLS_SSL_CACHE_H
POLARSSL_SSL_CBC_RECORD_SPLITTING MBEDTLS_SSL_CBC_RECORD_SPLITTING
POLARSSL_SSL_CIPHERSUITES_H MBEDTLS_SSL_CIPHERSUITES_H
POLARSSL_SSL_CLI_C MBEDTLS_SSL_CLI_C
POLARSSL_SSL_COOKIE_C MBEDTLS_SSL_COOKIE_C
POLARSSL_SSL_COOKIE_H MBEDTLS_SSL_COOKIE_H
POLARSSL_SSL_COOKIE_TIMEOUT MBEDTLS_SSL_COOKIE_TIMEOUT
POLARSSL_SSL_DEBUG_ALL MBEDTLS_SSL_DEBUG_ALL
POLARSSL_SSL_DISABLE_RENEGOTIATION MBEDTLS_SSL_DISABLE_RENEGOTIATION
POLARSSL_SSL_DTLS_ANTI_REPLAY MBEDTLS_SSL_DTLS_ANTI_REPLAY
POLARSSL_SSL_DTLS_BADMAC_LIMIT MBEDTLS_SSL_DTLS_BADMAC_LIMIT
POLARSSL_SSL_DTLS_HELLO_VERIFY MBEDTLS_SSL_DTLS_HELLO_VERIFY
POLARSSL_SSL_ENCRYPT_THEN_MAC MBEDTLS_SSL_ENCRYPT_THEN_MAC
POLARSSL_SSL_EXTENDED_MASTER_SECRET MBEDTLS_SSL_EXTENDED_MASTER_SECRET
POLARSSL_SSL_FALLBACK_SCSV MBEDTLS_SSL_FALLBACK_SCSV
POLARSSL_SSL_H
MBEDTLS_SSL_H
POLARSSL_SSL_HW_RECORD_ACCEL MBEDTLS_SSL_HW_RECORD_ACCEL
POLARSSL_SSL_MAX_FRAGMENT_LENGTH MBEDTLS_SSL_MAX_FRAGMENT_LENGTH
POLARSSL_SSL_PROTO_DTLS MBEDTLS_SSL_PROTO_DTLS
POLARSSL_SSL_PROTO_SSL3 MBEDTLS_SSL_PROTO_SSL3
POLARSSL_SSL_PROTO_TLS1 MBEDTLS_SSL_PROTO_TLS1
POLARSSL_SSL_PROTO_TLS1_1 MBEDTLS_SSL_PROTO_TLS1_1
POLARSSL_SSL_PROTO_TLS1_2 MBEDTLS_SSL_PROTO_TLS1_2
POLARSSL_SSL_RENEGOTIATION MBEDTLS_SSL_RENEGOTIATION
POLARSSL_SSL_SERVER_NAME_INDICATION MBEDTLS_SSL_SERVER_NAME_INDICATION
POLARSSL_SSL_SESSION_TICKETS MBEDTLS_SSL_SESSION_TICKETS
POLARSSL_SSL_SRV_C MBEDTLS_SSL_SRV_C
POLARSSL_SSL_SRV_RESPECT_CLIENT_PREFERENCE
MBEDTLS_SSL_SRV_RESPECT_CLIENT_PREFERENCE

POLARSSL_SSL_SRV_SUPPORT_SSLV2_CLIENT_HELLO
MBEDTLS_SSL_SRV_SUPPORT_SSLV2_CLIENT_HELLO
POLARSSL_SSL_TLS_C MBEDTLS_SSL_TLS_C
POLARSSL_SSL_TRUNCATED_HMAC MBEDTLS_SSL_TRUNCATED_HMAC
POLARSSL_THREADING_ALT MBEDTLS_THREADING_ALT
POLARSSL_THREADING_C MBEDTLS_THREADING_C
POLARSSL_THREADING_H MBEDTLS_THREADING_H
POLARSSL_THREADING_IMPL
MBEDTLS_THREADING_IMPL
POLARSSL_THREADING_PTHREAD MBEDTLS_THREADING_PTHREAD
POLARSSL_TIMING_ALT MBEDTLS_TIMING_ALT
POLARSSL_TIMING_C MBEDTLS_TIMING_C
POLARSSL_TIMING_H MBEDTLS_TIMING_H
POLARSSL_VERSION_C MBEDTLS_VERSION_C
POLARSSL_VERSION_FEATURES MBEDTLS_VERSION_FEATURES
POLARSSL_VERSION_H MBEDTLS_VERSION_H
POLARSSL_VERSION_MAJOR MBEDTLS_VERSION_MAJOR
POLARSSL_VERSION_MINOR MBEDTLS_VERSION_MINOR
POLARSSL_VERSION_NUMBER MBEDTLS_VERSION_NUMBER
POLARSSL_VERSION_PATCH MBEDTLS_VERSION_PATCH
POLARSSL_VERSION_STRING MBEDTLS_VERSION_STRING
POLARSSL_VERSION_STRING_FULL MBEDTLS_VERSION_STRING_FULL
POLARSSL_X509_ALLOW_EXTENSIONS_NON_V3 MBEDTLS_X509_ALLOW_EXTENSIONS_NON_V3
POLARSSL_X509_ALLOW_UNSUPPORTED_CRITICAL_EXTENSION
MBEDTLS_X509_ALLOW_UNSUPPORTED_CRITICAL_EXTENSION
POLARSSL_X509_CHECK_EXTENDED_KEY_USAGE
MBEDTLS_X509_CHECK_EXTENDED_KEY_USAGE
POLARSSL_X509_CHECK_KEY_USAGE MBEDTLS_X509_CHECK_KEY_USAGE
POLARSSL_X509_CREATE_C MBEDTLS_X509_CREATE_C
POLARSSL_X509_CRL_H MBEDTLS_X509_CRL_H
POLARSSL_X509_CRL_PARSE_C
MBEDTLS_X509_CRL_PARSE_C
POLARSSL_X509_CRT_H MBEDTLS_X509_CRT_H
POLARSSL_X509_CRT_PARSE_C MBEDTLS_X509_CRT_PARSE_C
POLARSSL_X509_CRT_WRITE_C MBEDTLS_X509_CRT_WRITE_C
POLARSSL_X509_CSR_H MBEDTLS_X509_CSR_H
POLARSSL_X509_CSR_PARSE_C MBEDTLS_X509_CSR_PARSE_C
POLARSSL_X509_CSR_WRITE_C MBEDTLS_X509_CSR_WRITE_C
POLARSSL_X509_H MBEDTLS_X509_H
POLARSSL_X509_MAX_INTERMEDIATE_CA MBEDTLS_X509_MAX_INTERMEDIATE_CA
POLARSSL_X509_RSASSA_PSS_SUPPORT MBEDTLS_X509_RSASSA_PSS_SUPPORT
POLARSSL_X509_USE_C MBEDTLS_X509_USE_C
POLARSSL_XTEA_ALT MBEDTLS_XTEA_ALT
POLARSSL_XTEA_C MBEDTLS_XTEA_C
POLARSSL_XTEA_H MBEDTLS_XTEA_H
POLARSSL_ZLIB_SUPPORT MBEDTLS_ZLIB_SUPPORT
RSA_CRYPT MBEDTLS_RSA_CRYPT
RSA_PKCS_V15 MBEDTLS_RSA_PKCS_V15

RSA_PKCS_V21 MBEDTLS_RSA_PKCS_V21
RSA_PRIVATE MBEDTLS_RSA_PRIVATE
RSA_PUBLIC MBEDTLS_RSA_PUBLIC
RSA_SALT_LEN_ANY MBEDTLS_RSA_SALT_LEN_ANY
RSA_SIGN MBEDTLS_RSA_SIGN
SSL_ALERT_LEVEL_FATAL MBEDTLS_SSL_ALERT_LEVEL_FATAL
SSL_ALERT_LEVEL_WARNING MBEDTLS_SSL_ALERT_LEVEL_WARNING
SSL_ALERT_MSG_ACCESS_DENIED
MBEDTLS_SSL_ALERT_MSG_ACCESS_DENIED
SSL_ALERT_MSG_BAD_CERT MBEDTLS_SSL_ALERT_MSG_BAD_CERT
SSL_ALERT_MSG_BAD_RECORD_MAC MBEDTLS_SSL_ALERT_MSG_BAD_RECORD_MAC
SSL_ALERT_MSG_CERT_EXPIRED MBEDTLS_SSL_ALERT_MSG_CERT_EXPIRED
SSL_ALERT_MSG_CERT_REVOKED MBEDTLS_SSL_ALERT_MSG_CERT_REVOKED
SSL_ALERT_MSG_CERT_UNKNOWN MBEDTLS_SSL_ALERT_MSG_CERT_UNKNOWN
SSL_ALERT_MSG_CLOSE_NOTIFY MBEDTLS_SSL_ALERT_MSG_CLOSE_NOTIFY
SSL_ALERT_MSG_DECODE_ERROR MBEDTLS_SSL_ALERT_MSG_DECODE_ERROR
SSL_ALERT_MSG_DECOMPRESSION_FAILURE
MBEDTLS_SSL_ALERT_MSG_DECOMPRESSION_FAILURE
SSL_ALERT_MSG_DECRYPTION_FAILED MBEDTLS_SSL_ALERT_MSG_DECRYPTION_FAILED
SSL_ALERT_MSG_DECRYPT_ERROR MBEDTLS_SSL_ALERT_MSG_DECRYPT_ERROR
SSL_ALERT_MSG_EXPORT_RESTRICTION MBEDTLS_SSL_ALERT_MSG_EXPORT_RESTRICTION
SSL_ALERT_MSG_HANDSHAKE_FAILURE MBEDTLS_SSL_ALERT_MSG_HANDSHAKE_FAILURE
SSL_ALERT_MSG_ILLEGAL_PARAMETER MBEDTLS_SSL_ALERT_MSG_ILLEGAL_PARAMETER
SSL_ALERT_MSG_INAPROPRIATE_FALLBACK
MBEDTLS_SSL_ALERT_MSG_INAPROPRIATE_FALLBACK
SSL_ALERT_MSG_INSUFFICIENT_SECURITY
MBEDTLS_SSL_ALERT_MSG_INSUFFICIENT_SECURITY
SSL_ALERT_MSG_INTERNAL_ERROR MBEDTLS_SSL_ALERT_MSG_INTERNAL_ERROR
SSL_ALERT_MSG_NO_APPLICATION_PROTOCOL
MBEDTLS_SSL_ALERT_MSG_NO_APPLICATION_PROTOCOL
SSL_ALERT_MSG_NO_CERT MBEDTLS_SSL_ALERT_MSG_NO_CERT
SSL_ALERT_MSG_NO_RENEGOTIATION MBEDTLS_SSL_ALERT_MSG_NO_RENEGOTIATION
SSL_ALERT_MSG_PROTOCOL_VERSION MBEDTLS_SSL_ALERT_MSG_PROTOCOL_VERSION
SSL_ALERT_MSG_RECORD_OVERFLOW MBEDTLS_SSL_ALERT_MSG_RECORD_OVERFLOW
SSL_ALERT_MSG_UNEXPECTED_MESSAGE MBEDTLS_SSL_ALERT_MSG_UNEXPECTED_MESSAGE
SSL_ALERT_MSG_UNKNOWN_CA MBEDTLS_SSL_ALERT_MSG_UNKNOWN_CA
SSL_ALERT_MSG_UNKNOWN_PSK_IDENTITY
MBEDTLS_SSL_ALERT_MSG_UNKNOWN_PSK_IDENTITY
SSL_ALERT_MSG_UNRECOGNIZED_NAME MBEDTLS_SSL_ALERT_MSG_UNRECOGNIZED_NAME
SSL_ALERT_MSG_UNSUPPORTED_CERT MBEDTLS_SSL_ALERT_MSG_UNSUPPORTED_CERT
SSL_ALERT_MSG_UNSUPPORTED_EXT MBEDTLS_SSL_ALERT_MSG_UNSUPPORTED_EXT
SSL_ALERT_MSG_USER_CANCELED MBEDTLS_SSL_ALERT_MSG_USER_CANCELED
SSL_ANTI_REPLAY_DISABLED
MBEDTLS_SSL_ANTI_REPLAY_DISABLED
SSL_ANTI_REPLAY_ENABLED MBEDTLS_SSL_ANTI_REPLAY_ENABLED
SSL_ARC4_DISABLED MBEDTLS_SSL_ARC4_DISABLED
SSL_ARC4_ENABLED MBEDTLS_SSL_ARC4_ENABLED
SSL_BUFFER_LEN MBEDTLS_SSL_BUFFER_LEN

SSL_CACHE_DEFAULT_MAX_ENTRIES MBEDTLS_SSL_CACHE_DEFAULT_MAX_ENTRIES
SSL_CACHE_DEFAULT_TIMEOUT MBEDTLS_SSL_CACHE_DEFAULT_TIMEOUT
SSL_CBC_RECORD_SPLITTING_DISABLED MBEDTLS_SSL_CBC_RECORD_SPLITTING_DISABLED
SSL_CBC_RECORD_SPLITTING_ENABLED MBEDTLS_SSL_CBC_RECORD_SPLITTING_ENABLED
SSL_CERTIFICATE_REQUEST MBEDTLS_SSL_CERTIFICATE_REQUEST
SSL_CERTIFICATE_VERIFY MBEDTLS_SSL_CERTIFICATE_VERIFY
SSL_CERT_TYPE_ECDSA_SIGN MBEDTLS_SSL_CERT_TYPE_ECDSA_SIGN
SSL_CERT_TYPE_RSA_SIGN MBEDTLS_SSL_CERT_TYPE_RSA_SIGN
SSL_CHANNEL_INBOUND MBEDTLS_SSL_CHANNEL_INBOUND
SSL_CHANNEL_OUTBOUND MBEDTLS_SSL_CHANNEL_OUTBOUND
SSL_CIPHERSUITES MBEDTLS_SSL_CIPHERSUITES
SSL_CLIENT_CERTIFICATE MBEDTLS_SSL_CLIENT_CERTIFICATE
SSL_CLIENT_CHANGE_CIPHER_SPEC MBEDTLS_SSL_CLIENT_CHANGE_CIPHER_SPEC
SSL_CLIENT_FINISHED
MBEDTLS_SSL_CLIENT_FINISHED
SSL_CLIENT_HELLO MBEDTLS_SSL_CLIENT_HELLO
SSL_CLIENT_KEY_EXCHANGE MBEDTLS_SSL_CLIENT_KEY_EXCHANGE
SSL_COMPRESSION_ADD MBEDTLS_SSL_COMPRESSION_ADD
SSL_COMPRESS_DEFLATE MBEDTLS_SSL_COMPRESS_DEFLATE
SSL_COMPRESS_NULL MBEDTLS_SSL_COMPRESS_NULL
SSL_DEBUG_BUF MBEDTLS_SSL_DEBUG_BUF
SSL_DEBUG_CRT MBEDTLS_SSL_DEBUG_CRT
SSL_DEBUG_ECP MBEDTLS_SSL_DEBUG_ECP
SSL_DEBUG_MPI MBEDTLS_SSL_DEBUG_MPI
SSL_DEBUG_MSG MBEDTLS_SSL_DEBUG_MSG
SSL_DEBUG_RET MBEDTLS_SSL_DEBUG_RET
SSL_DEFAULT_TICKET_LIFETIME MBEDTLS_SSL_DEFAULT_TICKET_LIFETIME
SSL_DTLS_TIMEOUT_DFL_MAX MBEDTLS_SSL_DTLS_TIMEOUT_DFL_MAX
SSL_DTLS_TIMEOUT_DFL_MIN MBEDTLS_SSL_DTLS_TIMEOUT_DFL_MIN
SSL_EMPTY_RENEGOTIATION_INFO MBEDTLS_SSL_EMPTY_RENEGOTIATION_INFO
SSL_ETM_DISABLED MBEDTLS_SSL_ETM_DISABLED
SSL_ETM_ENABLED MBEDTLS_SSL_ETM_ENABLED
SSL_EXTENDED_MS_DISABLED MBEDTLS_SSL_EXTENDED_MS_DISABLED
SSL_EXTENDED_MS_ENABLED MBEDTLS_SSL_EXTENDED_MS_ENABLED
SSL_FALLBACK_SCSV MBEDTLS_SSL_FALLBACK_SCSV
SSL_FLUSH_BUFFERS
MBEDTLS_SSL_FLUSH_BUFFERS
SSL_HANDSHAKE_OVER MBEDTLS_SSL_HANDSHAKE_OVER
SSL_HANDSHAKE_WRAPUP MBEDTLS_SSL_HANDSHAKE_WRAPUP
SSL_HASH_MD5 MBEDTLS_SSL_HASH_MD5
SSL_HASH_NONE MBEDTLS_SSL_HASH_NONE
SSL_HASH_SHA1 MBEDTLS_SSL_HASH_SHA1
SSL_HASH_SHA224 MBEDTLS_SSL_HASH_SHA224
SSL_HASH_SHA256 MBEDTLS_SSL_HASH_SHA256
SSL_HASH_SHA384 MBEDTLS_SSL_HASH_SHA384
SSL_HASH_SHA512 MBEDTLS_SSL_HASH_SHA512
SSL_HELLO_REQUEST MBEDTLS_SSL_HELLO_REQUEST
SSL_HS_CERTIFICATE MBEDTLS_SSL_HS_CERTIFICATE

SSL_HS_CERTIFICATE_REQUEST MBEDTLS_SSL_HS_CERTIFICATE_REQUEST
SSL_HS_CERTIFICATE_VERIFY MBEDTLS_SSL_HS_CERTIFICATE_VERIFY
SSL_HS_CLIENT_HELLO MBEDTLS_SSL_HS_CLIENT_HELLO
SSL_HS_CLIENT_KEY_EXCHANGE MBEDTLS_SSL_HS_CLIENT_KEY_EXCHANGE
SSL_HS_FINISHED MBEDTLS_SSL_HS_FINISHED
SSL_HS_HELLO_REQUEST MBEDTLS_SSL_HS_HELLO_REQUEST
SSL_HS_HELLO_VERIFY_REQUEST MBEDTLS_SSL_HS_HELLO_VERIFY_REQUEST
SSL_HS_NEW_SESSION_TICKET MBEDTLS_SSL_HS_NEW_SESSION_TICKET
SSL_HS_SERVER_HELLO MBEDTLS_SSL_HS_SERVER_HELLO
SSL_HS_SERVER_HELLO_DONE
MBEDTLS_SSL_HS_SERVER_HELLO_DONE
SSL_HS_SERVER_KEY_EXCHANGE MBEDTLS_SSL_HS_SERVER_KEY_EXCHANGE
SSL_INITIAL_HANDSHAKE MBEDTLS_SSL_INITIAL_HANDSHAKE
SSL_IS_CLIENT MBEDTLS_SSL_IS_CLIENT
SSL_IS_FALLBACK MBEDTLS_SSL_IS_FALLBACK
SSL_IS_NOT_FALLBACK MBEDTLS_SSL_IS_NOT_FALLBACK
SSL_IS_SERVER MBEDTLS_SSL_IS_SERVER
SSL_LEGACY_ALLOW_RENEGOTIATION MBEDTLS_SSL_LEGACY_ALLOW_RENEGOTIATION
SSL_LEGACY_BREAK_HANDSHAKE MBEDTLS_SSL_LEGACY_BREAK_HANDSHAKE
SSL_LEGACY_NO_RENEGOTIATION MBEDTLS_SSL_LEGACY_NO_RENEGOTIATION
SSL_LEGACY_RENEGOTIATION MBEDTLS_SSL_LEGACY_RENEGOTIATION
SSL_MAC_ADD MBEDTLS_SSL_MAC_ADD
SSL_MAJOR_VERSION_3 MBEDTLS_SSL_MAJOR_VERSION_3
SSL_MAX_CONTENT_LEN MBEDTLS_SSL_MAX_CONTENT_LEN
SSL_MAX_FRAG_LEN_1024 MBEDTLS_SSL_MAX_FRAG_LEN_1024
SSL_MAX_FRAG_LEN_2048 MBEDTLS_SSL_MAX_FRAG_LEN_2048
SSL_MAX_FRAG_LEN_4096 MBEDTLS_SSL_MAX_FRAG_LEN_4096
SSL_MAX_FRAG_LEN_512 MBEDTLS_SSL_MAX_FRAG_LEN_512
SSL_MAX_FRAG_LEN_INVALID MBEDTLS_SSL_MAX_FRAG_LEN_INVALID
SSL_MAX_FRAG_LEN_NONE MBEDTLS_SSL_MAX_FRAG_LEN_NONE
SSL_MAX_MAJOR_VERSION
MBEDTLS_SSL_MAX_MAJOR_VERSION
SSL_MAX_MINOR_VERSION MBEDTLS_SSL_MAX_MINOR_VERSION
SSL_MINOR_VERSION_0 MBEDTLS_SSL_MINOR_VERSION_0
SSL_MINOR_VERSION_1 MBEDTLS_SSL_MINOR_VERSION_1
SSL_MINOR_VERSION_2 MBEDTLS_SSL_MINOR_VERSION_2
SSL_MINOR_VERSION_3 MBEDTLS_SSL_MINOR_VERSION_3
SSL_MIN_MAJOR_VERSION MBEDTLS_SSL_MIN_MAJOR_VERSION
SSL_MIN_MINOR_VERSION MBEDTLS_SSL_MIN_MINOR_VERSION
SSL_MSG_ALERT MBEDTLS_SSL_MSG_ALERT
SSL_MSG_APPLICATION_DATA MBEDTLS_SSL_MSG_APPLICATION_DATA
SSL_MSG_CHANGE_CIPHER_SPEC MBEDTLS_SSL_MSG_CHANGE_CIPHER_SPEC
SSL_MSG_HANDSHAKE MBEDTLS_SSL_MSG_HANDSHAKE
SSL_PADDING_ADD MBEDTLS_SSL_PADDING_ADD
SSL_RENEGOTIATION MBEDTLS_SSL_RENEGOTIATION
SSL_RENEGOTIATION_DISABLED MBEDTLS_SSL_RENEGOTIATION_DISABLED
SSL_RENEGOTIATION_DONE MBEDTLS_SSL_RENEGOTIATION_DONE
SSL_RENEGOTIATION_ENABLED MBEDTLS_SSL_RENEGOTIATION_ENABLED

SSL_RENEGOTIATION_NOT_ENFORCED MBEDTLS_SSL_RENEGOTIATION_NOT_ENFORCED
SSL_RENEGOTIATION_PENDING MBEDTLS_SSL_RENEGOTIATION_PENDING
SSL_RENEGO_MAX_RECORDS_DEFAULT
MBEDTLS_SSL_RENEGO_MAX_RECORDS_DEFAULT
SSL_RETRANS_FINISHED MBEDTLS_SSL_RETRANS_FINISHED
SSL_RETRANS_PREPARING MBEDTLS_SSL_RETRANS_PREPARING
SSL_RETRANS_SENDING MBEDTLS_SSL_RETRANS_SENDING
SSL_RETRANS_WAITING MBEDTLS_SSL_RETRANS_WAITING
SSL_SECURE_RENEGOTIATION MBEDTLS_SSL_SECURE_RENEGOTIATION
SSL_SERVER_CERTIFICATE MBEDTLS_SSL_SERVER_CERTIFICATE
SSL_SERVER_CHANGE_CIPHER_SPEC MBEDTLS_SSL_SERVER_CHANGE_CIPHER_SPEC
SSL_SERVER_FINISHED MBEDTLS_SSL_SERVER_FINISHED
SSL_SERVER_HELLO MBEDTLS_SSL_SERVER_HELLO
SSL_SERVER_HELLO_DONE MBEDTLS_SSL_SERVER_HELLO_DONE
SSL_SERVER_HELLO_VERIFY_REQUEST_SENT
MBEDTLS_SSL_SERVER_HELLO_VERIFY_REQUEST_SENT
SSL_SERVER_KEY_EXCHANGE MBEDTLS_SSL_SERVER_KEY_EXCHANGE
SSL_SERVER_NEW_SESSION_TICKET MBEDTLS_SSL_SERVER_NEW_SESSION_TICKET
SSL_SESSION_TICKETS_DISABLED MBEDTLS_SSL_SESSION_TICKETS_DISABLED
SSL_SESSION_TICKETS_ENABLED MBEDTLS_SSL_SESSION_TICKETS_ENABLED
SSL_SIG_ANON MBEDTLS_SSL_SIG_ANON
SSL_SIG_ECDSA MBEDTLS_SSL_SIG_ECDSA
SSL_SIG_RSA
MBEDTLS_SSL_SIG_RSA
SSL_TRANSPORT_DATAGRAM MBEDTLS_SSL_TRANSPORT_DATAGRAM
SSL_TRANSPORT_STREAM MBEDTLS_SSL_TRANSPORT_STREAM
SSL_TRUNCATED_HMAC_LEN MBEDTLS_SSL_TRUNCATED_HMAC_LEN
SSL_TRUNC_HMAC_DISABLED MBEDTLS_SSL_TRUNC_HMAC_DISABLED
SSL_TRUNC_HMAC_ENABLED MBEDTLS_SSL_TRUNC_HMAC_ENABLED
SSL_VERIFY_DATA_MAX_LEN MBEDTLS_SSL_VERIFY_DATA_MAX_LEN
SSL_VERIFY_NONE MBEDTLS_SSL_VERIFY_NONE
SSL_VERIFY_OPTIONAL MBEDTLS_SSL_VERIFY_OPTIONAL
SSL_VERIFY_REQUIRED MBEDTLS_SSL_VERIFY_REQUIRED
TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA MBEDTLS_TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA
TLS_DHE_PSK_WITH_AES_128_CBC_SHA MBEDTLS_TLS_DHE_PSK_WITH_AES_128_CBC_SHA
TLS_DHE_PSK_WITH_AES_128_CBC_SHA256 MBEDTLS_TLS_DHE_PSK_WITH_AES_128_CBC_SHA256
TLS_DHE_PSK_WITH_AES_128_CCM MBEDTLS_TLS_DHE_PSK_WITH_AES_128_CCM
TLS_DHE_PSK_WITH_AES_128_CCM_8 MBEDTLS_TLS_DHE_PSK_WITH_AES_128_CCM_8
TLS_DHE_PSK_WITH_AES_128_GCM_SHA256
MBEDTLS_TLS_DHE_PSK_WITH_AES_128_GCM_SHA256
TLS_DHE_PSK_WITH_AES_256_CBC_SHA MBEDTLS_TLS_DHE_PSK_WITH_AES_256_CBC_SHA
TLS_DHE_PSK_WITH_AES_256_CBC_SHA384
MBEDTLS_TLS_DHE_PSK_WITH_AES_256_CBC_SHA384
TLS_DHE_PSK_WITH_AES_256_CCM MBEDTLS_TLS_DHE_PSK_WITH_AES_256_CCM
TLS_DHE_PSK_WITH_AES_256_CCM_8 MBEDTLS_TLS_DHE_PSK_WITH_AES_256_CCM_8
TLS_DHE_PSK_WITH_AES_256_GCM_SHA384
MBEDTLS_TLS_DHE_PSK_WITH_AES_256_GCM_SHA384
TLS_DHE_PSK_WITH_CAMELLIA_128_CBC_SHA256

MBEDTLS_TLS_DHE_PSK_WITH_CAMELLIA_128_CBC_SHA256
TLS_DHE_PSK_WITH_CAMELLIA_128_GCM_SHA256
MBEDTLS_TLS_DHE_PSK_WITH_CAMELLIA_128_GCM_SHA256
TLS_DHE_PSK_WITH_CAMELLIA_256_CBC_SHA384
MBEDTLS_TLS_DHE_PSK_WITH_CAMELLIA_256_CBC_SHA384
TLS_DHE_PSK_WITH_CAMELLIA_256_GCM_SHA384
MBEDTLS_TLS_DHE_PSK_WITH_CAMELLIA_256_GCM_SHA384
TLS_DHE_PSK_WITH_NULL_SHA MBEDTLS_TLS_DHE_PSK_WITH_NULL_SHA
TLS_DHE_PSK_WITH_NULL_SHA256 MBEDTLS_TLS_DHE_PSK_WITH_NULL_SHA256
TLS_DHE_PSK_WITH_NULL_SHA384 MBEDTLS_TLS_DHE_PSK_WITH_NULL_SHA384
TLS_DHE_PSK_WITH_RC4_128_SHA MBEDTLS_TLS_DHE_PSK_WITH_RC4_128_SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA MBEDTLS_TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
MBEDTLS_TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
MBEDTLS_TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CCM MBEDTLS_TLS_DHE_RSA_WITH_AES_128_CCM
TLS_DHE_RSA_WITH_AES_128_CCM_8 MBEDTLS_TLS_DHE_RSA_WITH_AES_128_CCM_8
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
MBEDTLS_TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA MBEDTLS_TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
MBEDTLS_TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CCM MBEDTLS_TLS_DHE_RSA_WITH_AES_256_CCM
TLS_DHE_RSA_WITH_AES_256_CCM_8 MBEDTLS_TLS_DHE_RSA_WITH_AES_256_CCM_8
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
MBEDTLS_TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
MBEDTLS_TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
MBEDTLS_TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256
MBEDTLS_TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
MBEDTLS_TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
MBEDTLS_TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384
MBEDTLS_TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384
TLS_DHE_RSA_WITH_DES_CBC_SHA MBEDTLS_TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
MBEDTLS_TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
MBEDTLS_TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
MBEDTLS_TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CCM MBEDTLS_TLS_ECDHE_ECDSA_WITH_AES_128_CCM
TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 MBEDTLS_TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
MBEDTLS_TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
MBEDTLS_TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
MBEDTLS_TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_CCM
MBEDTLS_TLS_ECDHE_ECDSA_WITH_AES_256_CCM
TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8 MBEDTLS_TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
MBEDTLS_TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256
MBEDTLS_TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256
MBEDTLS_TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384
MBEDTLS_TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384
MBEDTLS_TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_NULL_SHA MBEDTLS_TLS_ECDHE_ECDSA_WITH_NULL_SHA
TLS_ECDHE_ECDSA_WITH_RC4_128_SHA MBEDTLS_TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
TLS_ECDHE_PSK_WITH_3DES_EDE_CBC_SHA
MBEDTLS_TLS_ECDHE_PSK_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA MBEDTLS_TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA
TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256
MBEDTLS_TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256
TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA
MBEDTLS_TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA
TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384
MBEDTLS_TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384
TLS_ECDHE_PSK_WITH_CAMELLIA_128_CBC_SHA256
MBEDTLS_TLS_ECDHE_PSK_WITH_CAMELLIA_128_CBC_SHA256
TLS_ECDHE_PSK_WITH_CAMELLIA_256_CBC_SHA384
MBEDTLS_TLS_ECDHE_PSK_WITH_CAMELLIA_256_CBC_SHA384
TLS_ECDHE_PSK_WITH_NULL_SHA MBEDTLS_TLS_ECDHE_PSK_WITH_NULL_SHA
TLS_ECDHE_PSK_WITH_NULL_SHA256 MBEDTLS_TLS_ECDHE_PSK_WITH_NULL_SHA256
TLS_ECDHE_PSK_WITH_NULL_SHA384 MBEDTLS_TLS_ECDHE_PSK_WITH_NULL_SHA384
TLS_ECDHE_PSK_WITH_RC4_128_SHA MBEDTLS_TLS_ECDHE_PSK_WITH_RC4_128_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
MBEDTLS_TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA MBEDTLS_TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
MBEDTLS_TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
MBEDTLS_TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA MBEDTLS_TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

MBEDTLS_TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
MBEDTLS_TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
MBEDTLS_TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256
MBEDTLS_TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
MBEDTLS_TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384
MBEDTLS_TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_NULL_SHA MBEDTLS_TLS_ECDHE_RSA_WITH_NULL_SHA
TLS_ECDHE_RSA_WITH_RC4_128_SHA MBEDTLS_TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
MBEDTLS_TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
MBEDTLS_TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
MBEDTLS_TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
MBEDTLS_TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
MBEDTLS_TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
MBEDTLS_TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
MBEDTLS_TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_ECDSA_WITH_CAMELLIA_128_CBC_SHA256
MBEDTLS_TLS_ECDH_ECDSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_ECDH_ECDSA_WITH_CAMELLIA_128_GCM_SHA256
MBEDTLS_TLS_ECDH_ECDSA_WITH_CAMELLIA_128_GCM_SHA256
TLS_ECDH_ECDSA_WITH_CAMELLIA_256_CBC_SHA384
MBEDTLS_TLS_ECDH_ECDSA_WITH_CAMELLIA_256_CBC_SHA384
TLS_ECDH_ECDSA_WITH_CAMELLIA_256_GCM_SHA384
MBEDTLS_TLS_ECDH_ECDSA_WITH_CAMELLIA_256_GCM_SHA384
TLS_ECDH_ECDSA_WITH_NULL_SHA MBEDTLS_TLS_ECDH_ECDSA_WITH_NULL_SHA
TLS_ECDH_ECDSA_WITH_RC4_128_SHA MBEDTLS_TLS_ECDH_ECDSA_WITH_RC4_128_SHA
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
MBEDTLS_TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA MBEDTLS_TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
MBEDTLS_TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
MBEDTLS_TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA MBEDTLS_TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
MBEDTLS_TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384

MBEDTLS_TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_RSA_WITH_CAMELLIA_128_CBC_SHA256
MBEDTLS_TLS_ECDH_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_ECDH_RSA_WITH_CAMELLIA_128_GCM_SHA256
MBEDTLS_TLS_ECDH_RSA_WITH_CAMELLIA_128_GCM_SHA256
TLS_ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA384
MBEDTLS_TLS_ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA384
TLS_ECDH_RSA_WITH_CAMELLIA_256_GCM_SHA384
MBEDTLS_TLS_ECDH_RSA_WITH_CAMELLIA_256_GCM_SHA384
TLS_ECDH_RSA_WITH_NULL_SHA MBEDTLS_TLS_ECDH_RSA_WITH_NULL_SHA
TLS_ECDH_RSA_WITH_RC4_128_SHA MBEDTLS_TLS_ECDH_RSA_WITH_RC4_128_SHA
TLS_EXT_ALPN MBEDTLS_TLS_EXT_ALPN
TLS_EXT_ENCRYPT_THEN_MAC MBEDTLS_TLS_EXT_ENCRYPT_THEN_MAC
TLS_EXT_EXTENDED_MASTER_SECRET
MBEDTLS_TLS_EXT_EXTENDED_MASTER_SECRET
TLS_EXT_MAX_FRAGMENT_LENGTH MBEDTLS_TLS_EXT_MAX_FRAGMENT_LENGTH
TLS_EXT_RENEGOTIATION_INFO MBEDTLS_TLS_EXT_RENEGOTIATION_INFO
TLS_EXT_SERVERNAME MBEDTLS_TLS_EXT_SERVERNAME
TLS_EXT_SERVERNAME_HOSTNAME MBEDTLS_TLS_EXT_SERVERNAME_HOSTNAME
TLS_EXT_SESSION_TICKET MBEDTLS_TLS_EXT_SESSION_TICKET
TLS_EXT_SIG_ALG MBEDTLS_TLS_EXT_SIG_ALG
TLS_EXT_SUPPORTED_ELLIPTIC_CURVES MBEDTLS_TLS_EXT_SUPPORTED_ELLIPTIC_CURVES
TLS_EXT_SUPPORTED_POINT_FORMATS MBEDTLS_TLS_EXT_SUPPORTED_POINT_FORMATS
TLS_EXT_SUPPORTED_POINT_FORMATS_PRESENT
MBEDTLS_TLS_EXT_SUPPORTED_POINT_FORMATS_PRESENT
TLS_EXT_TRUNCATED_HMAC MBEDTLS_TLS_EXT_TRUNCATED_HMAC
TLS_PSK_WITH_3DES_EDE_CBC_SHA MBEDTLS_TLS_PSK_WITH_3DES_EDE_CBC_SHA
TLS_PSK_WITH_AES_128_CBC_SHA MBEDTLS_TLS_PSK_WITH_AES_128_CBC_SHA
TLS_PSK_WITH_AES_128_CBC_SHA256 MBEDTLS_TLS_PSK_WITH_AES_128_CBC_SHA256
TLS_PSK_WITH_AES_128_CCM MBEDTLS_TLS_PSK_WITH_AES_128_CCM
TLS_PSK_WITH_AES_128_CCM_8 MBEDTLS_TLS_PSK_WITH_AES_128_CCM_8
TLS_PSK_WITH_AES_128_GCM_SHA256
MBEDTLS_TLS_PSK_WITH_AES_128_GCM_SHA256
TLS_PSK_WITH_AES_256_CBC_SHA MBEDTLS_TLS_PSK_WITH_AES_256_CBC_SHA
TLS_PSK_WITH_AES_256_CBC_SHA384 MBEDTLS_TLS_PSK_WITH_AES_256_CBC_SHA384
TLS_PSK_WITH_AES_256_CCM MBEDTLS_TLS_PSK_WITH_AES_256_CCM
TLS_PSK_WITH_AES_256_CCM_8 MBEDTLS_TLS_PSK_WITH_AES_256_CCM_8
TLS_PSK_WITH_AES_256_GCM_SHA384 MBEDTLS_TLS_PSK_WITH_AES_256_GCM_SHA384
TLS_PSK_WITH_CAMELLIA_128_CBC_SHA256
MBEDTLS_TLS_PSK_WITH_CAMELLIA_128_CBC_SHA256
TLS_PSK_WITH_CAMELLIA_128_GCM_SHA256
MBEDTLS_TLS_PSK_WITH_CAMELLIA_128_GCM_SHA256
TLS_PSK_WITH_CAMELLIA_256_CBC_SHA384
MBEDTLS_TLS_PSK_WITH_CAMELLIA_256_CBC_SHA384
TLS_PSK_WITH_CAMELLIA_256_GCM_SHA384
MBEDTLS_TLS_PSK_WITH_CAMELLIA_256_GCM_SHA384
TLS_PSK_WITH_NULL_SHA MBEDTLS_TLS_PSK_WITH_NULL_SHA
TLS_PSK_WITH_NULL_SHA256 MBEDTLS_TLS_PSK_WITH_NULL_SHA256

TLS_PSK_WITH_NULL_SHA384 MBEDTLS_TLS_PSK_WITH_NULL_SHA384
TLS_PSK_WITH_RC4_128_SHA MBEDTLS_TLS_PSK_WITH_RC4_128_SHA
TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA MBEDTLS_TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA
TLS_RSA_PSK_WITH_AES_128_CBC_SHA
MBEDTLS_TLS_RSA_PSK_WITH_AES_128_CBC_SHA
TLS_RSA_PSK_WITH_AES_128_CBC_SHA256 MBEDTLS_TLS_RSA_PSK_WITH_AES_128_CBC_SHA256
TLS_RSA_PSK_WITH_AES_128_GCM_SHA256
MBEDTLS_TLS_RSA_PSK_WITH_AES_128_GCM_SHA256
TLS_RSA_PSK_WITH_AES_256_CBC_SHA MBEDTLS_TLS_RSA_PSK_WITH_AES_256_CBC_SHA
TLS_RSA_PSK_WITH_AES_256_CBC_SHA384 MBEDTLS_TLS_RSA_PSK_WITH_AES_256_CBC_SHA384
TLS_RSA_PSK_WITH_AES_256_GCM_SHA384
MBEDTLS_TLS_RSA_PSK_WITH_AES_256_GCM_SHA384
TLS_RSA_PSK_WITH_CAMELLIA_128_CBC_SHA256
MBEDTLS_TLS_RSA_PSK_WITH_CAMELLIA_128_CBC_SHA256
TLS_RSA_PSK_WITH_CAMELLIA_128_GCM_SHA256
MBEDTLS_TLS_RSA_PSK_WITH_CAMELLIA_128_GCM_SHA256
TLS_RSA_PSK_WITH_CAMELLIA_256_CBC_SHA384
MBEDTLS_TLS_RSA_PSK_WITH_CAMELLIA_256_CBC_SHA384
TLS_RSA_PSK_WITH_CAMELLIA_256_GCM_SHA384
MBEDTLS_TLS_RSA_PSK_WITH_CAMELLIA_256_GCM_SHA384
TLS_RSA_PSK_WITH_NULL_SHA MBEDTLS_TLS_RSA_PSK_WITH_NULL_SHA
TLS_RSA_PSK_WITH_NULL_SHA256 MBEDTLS_TLS_RSA_PSK_WITH_NULL_SHA256
TLS_RSA_PSK_WITH_NULL_SHA384
MBEDTLS_TLS_RSA_PSK_WITH_NULL_SHA384
TLS_RSA_PSK_WITH_RC4_128_SHA MBEDTLS_TLS_RSA_PSK_WITH_RC4_128_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA MBEDTLS_TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA MBEDTLS_TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256 MBEDTLS_TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CCM MBEDTLS_TLS_RSA_WITH_AES_128_CCM
TLS_RSA_WITH_AES_128_CCM_8 MBEDTLS_TLS_RSA_WITH_AES_128_CCM_8
TLS_RSA_WITH_AES_128_GCM_SHA256 MBEDTLS_TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA MBEDTLS_TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256 MBEDTLS_TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_CCM MBEDTLS_TLS_RSA_WITH_AES_256_CCM
TLS_RSA_WITH_AES_256_CCM_8 MBEDTLS_TLS_RSA_WITH_AES_256_CCM_8
TLS_RSA_WITH_AES_256_GCM_SHA384 MBEDTLS_TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA MBEDTLS_TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
MBEDTLS_TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256
MBEDTLS_TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA MBEDTLS_TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
MBEDTLS_TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384
MBEDTLS_TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384
TLS_RSA_WITH_DES_CBC_SHA MBEDTLS_TLS_RSA_WITH_DES_CBC_SHA
TLS_RSA_WITH_NULL_MD5 MBEDTLS_TLS_RSA_WITH_NULL_MD5

TLS_RSA_WITH_NULL_SHA MBEDTLS_TLS_RSA_WITH_NULL_SHA
TLS_RSA_WITH_NULL_SHA256 MBEDTLS_TLS_RSA_WITH_NULL_SHA256
TLS_RSA_WITH_RC4_128_MD5 MBEDTLS_TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA MBEDTLS_TLS_RSA_WITH_RC4_128_SHA
X509_CRT_VERSION_1 MBEDTLS_X509_CRT_VERSION_1
X509_CRT_VERSION_2 MBEDTLS_X509_CRT_VERSION_2
X509_CRT_VERSION_3 MBEDTLS_X509_CRT_VERSION_3
X509_FORMAT_DER MBEDTLS_X509_FORMAT_DER
X509_FORMAT_PEM MBEDTLS_X509_FORMAT_PEM
X509_MAX_DN_NAME_SIZE MBEDTLS_X509_MAX_DN_NAME_SIZE
X509_RFC5280_MAX_SERIAL_LEN MBEDTLS_X509_RFC5280_MAX_SERIAL_LEN
X509_RFC5280_UTC_TIME_LEN
MBEDTLS_X509_RFC5280_UTC_TIME_LEN
XTEA_DECRYPT MBEDTLS_XTEA_DECRYPT
XTEA_ENCRYPT MBEDTLS_XTEA_ENCRYPT
_asn1_bitstring mbedtls_asn1_bitstring
_asn1_buf mbedtls_asn1_buf
_asn1_named_data mbedtls_asn1_named_data
_asn1_sequence mbedtls_asn1_sequence
_ssl_cache_context mbedtls_ssl_cache_context
_ssl_cache_entry mbedtls_ssl_cache_entry
_ssl_ciphersuite_t mbedtls_ssl_ciphersuite_t
_ssl_context mbedtls_ssl_context
_ssl_flight_item mbedtls_ssl_flight_item
_ssl_handshake_params mbedtls_ssl_handshake_params
_ssl_key_cert mbedtls_ssl_key_cert
_ssl_premaster_secret mbedtls_ssl_premaster_secret
_ssl_session mbedtls_ssl_session
_ssl_ticket_keys mbedtls_ssl_ticket_keys
_ssl_transform mbedtls_ssl_transform
_x509_crl mbedtls_x509_crl
_x509_crl_entry mbedtls_x509_crl_entry
_x509_crt mbedtls_x509_crt
_x509_csr mbedtls_x509_csr
_x509_time mbedtls_x509_time
_x509write_cert mbedtls_x509write_cert
_x509write_csr mbedtls_x509write_csr
aes_context mbedtls_aes_context
aes_crypt_cbc mbedtls_aes_crypt_cbc
aes_crypt_cfb128
mbedtls_aes_crypt_cfb128
aes_crypt_cfb8 mbedtls_aes_crypt_cfb8
aes_crypt_ctr mbedtls_aes_crypt_ctr
aes_crypt_ecb mbedtls_aes_crypt_ecb
aes_free mbedtls_aes_free
aes_init mbedtls_aes_init
aes_self_test mbedtls_aes_self_test
aes_setkey_dec mbedtls_aes_setkey_dec

aes_setkey_enc mbedtls_aes_setkey_enc
aesni_crypt_ecb mbedtls_aesni_crypt_ecb
aesni_gcm_mult mbedtls_aesni_gcm_mult
aesni_inverse_key mbedtls_aesni_inverse_key
aesni_setkey_enc mbedtls_aesni_setkey_enc
aesni_supports mbedtls_aesni_has_support
alarmed mbedtls_timing_alarmed
arc4_context mbedtls_arc4_context
arc4_crypt mbedtls_arc4_crypt
arc4_free mbedtls_arc4_free
arc4_init mbedtls_arc4_init
arc4_self_test mbedtls_arc4_self_test
arc4_setup mbedtls_arc4_setup
asn1_bitstring mbedtls_asn1_bitstring
asn1_buf mbedtls_asn1_buf
asn1_find_named_data mbedtls_asn1_find_named_data
asn1_free_named_data mbedtls_asn1_free_named_data
asn1_free_named_data_list mbedtls_asn1_free_named_data_list
asn1_get_alg mbedtls_asn1_get_alg
asn1_get_alg_null
mbedtls_asn1_get_alg_null
asn1_get_bitstring mbedtls_asn1_get_bitstring
asn1_get_bitstring_null mbedtls_asn1_get_bitstring_null
asn1_get_bool mbedtls_asn1_get_bool
asn1_get_int mbedtls_asn1_get_int
asn1_get_len mbedtls_asn1_get_len
asn1_get_mpi mbedtls_asn1_get_mpi
asn1_get_sequence_of mbedtls_asn1_get_sequence_of
asn1_get_tag mbedtls_asn1_get_tag
asn1_named_data mbedtls_asn1_named_data
asn1_sequence mbedtls_asn1_sequence
asn1_store_named_data mbedtls_asn1_store_named_data
asn1_write_algorithm_identifier mbedtls_asn1_write_algorithm_identifier
asn1_write_bitstring mbedtls_asn1_write_bitstring
asn1_write_bool mbedtls_asn1_write_bool
asn1_write_ia5_string mbedtls_asn1_write_ia5_string
asn1_write_int mbedtls_asn1_write_int
asn1_write_len mbedtls_asn1_write_len
asn1_write_mpi mbedtls_asn1_write_mpi
asn1_write_null mbedtls_asn1_write_null
asn1_write_octet_string mbedtls_asn1_write_octet_string
asn1_write_oid mbedtls_asn1_write_oid
asn1_write_printable_string mbedtls_asn1_write_printable_string
asn1_write_raw_buffer
mbedtls_asn1_write_raw_buffer
asn1_write_tag mbedtls_asn1_write_tag
base64_decode mbedtls_base64_decode
base64_encode mbedtls_base64_encode

base64_self_test mbedtls_base64_self_test
blowfish_context mbedtls_blowfish_context
blowfish_crypt_cbc mbedtls_blowfish_crypt_cbc
blowfish_crypt_cfb64 mbedtls_blowfish_crypt_cfb64
blowfish_crypt_ctr mbedtls_blowfish_crypt_ctr
blowfish_crypt_ecb mbedtls_blowfish_crypt_ecb
blowfish_free mbedtls_blowfish_free
blowfish_init mbedtls_blowfish_init
blowfish_setkey mbedtls_blowfish_setkey
camellia_context mbedtls_camellia_context
camellia_crypt_cbc mbedtls_camellia_crypt_cbc
camellia_crypt_cfb128 mbedtls_camellia_crypt_cfb128
camellia_crypt_ctr mbedtls_camellia_crypt_ctr
camellia_crypt_ecb mbedtls_camellia_crypt_ecb
camellia_free mbedtls_camellia_free
camellia_init mbedtls_camellia_init
camellia_self_test mbedtls_camellia_self_test
camellia_setkey_dec mbedtls_camellia_setkey_dec
camellia_setkey_enc mbedtls_camellia_setkey_enc
ccm_auth_decrypt
mbedtls_ccm_auth_decrypt
ccm_context mbedtls_ccm_context
ccm_encrypt_and_tag mbedtls_ccm_encrypt_and_tag
ccm_free mbedtls_ccm_free
ccm_init mbedtls_ccm_init
ccm_self_test mbedtls_ccm_self_test
cipher_auth_decrypt mbedtls_cipher_auth_decrypt
cipher_auth_encrypt mbedtls_cipher_auth_encrypt
cipher_base_t mbedtls_cipher_base_t
cipher_check_tag mbedtls_cipher_check_tag
cipher_context_t mbedtls_cipher_context_t
cipher_crypt mbedtls_cipher_crypt
cipher_definition_t mbedtls_cipher_definition_t
cipher_definitions mbedtls_cipher_definitions
cipher_finish mbedtls_cipher_finish
cipher_free mbedtls_cipher_free
cipher_free_ctx mbedtls_cipher_free_ctx
cipher_get_block_size mbedtls_cipher_get_block_size
cipher_get_cipher_mode mbedtls_cipher_get_cipher_mode
cipher_get_iv_size mbedtls_cipher_get_iv_size
cipher_get_key_size mbedtls_cipher_get_key_bitlen
cipher_get_name mbedtls_cipher_get_name
cipher_get_operation mbedtls_cipher_get_operation
cipher_get_type mbedtls_cipher_get_type
cipher_id_t
mbedtls_cipher_id_t
cipher_info_from_string mbedtls_cipher_info_from_string
cipher_info_from_type mbedtls_cipher_info_from_type

cipher_info_from_values mbedtls_cipher_info_from_values
cipher_info_t mbedtls_cipher_info_t
cipher_init mbedtls_cipher_init
cipher_init_ctx mbedtls_cipher_setup
cipher_list mbedtls_cipher_list
cipher_mode_t mbedtls_cipher_mode_t
cipher_padding_t mbedtls_cipher_padding_t
cipher_reset mbedtls_cipher_reset
cipher_self_test mbedtls_cipher_self_test
cipher_set_iv mbedtls_cipher_set_iv
cipher_set_padding_mode mbedtls_cipher_set_padding_mode
cipher_setkey mbedtls_cipher_setkey
cipher_type_t mbedtls_cipher_type_t
cipher_update mbedtls_cipher_update
cipher_update_ad mbedtls_cipher_update_ad
cipher_write_tag mbedtls_cipher_write_tag
ctr_drbg_context mbedtls_ctr_drbg_context
ctr_drbg_free mbedtls_ctr_drbg_free
ctr_drbg_init mbedtls_ctr_drbg_init
ctr_drbg_init_entropy_len mbedtls_ctr_drbg_init_entropy_len
ctr_drbg_random mbedtls_ctr_drbg_random
ctr_drbg_random_with_add
mbedtls_ctr_drbg_random_with_add
ctr_drbg_reseed mbedtls_ctr_drbg_reseed
ctr_drbg_self_test mbedtls_ctr_drbg_self_test
ctr_drbg_set_entropy_len mbedtls_ctr_drbg_set_entropy_len
ctr_drbg_set_prediction_resistance mbedtls_ctr_drbg_set_prediction_resistance
ctr_drbg_set_reseed_interval mbedtls_ctr_drbg_set_reseed_interval
ctr_drbg_update mbedtls_ctr_drbg_update
ctr_drbg_update_seed_file mbedtls_ctr_drbg_update_seed_file
ctr_drbg_write_seed_file mbedtls_ctr_drbg_write_seed_file
debug_fmt mbedtls_debug_fmt
debug_print_buf mbedtls_debug_print_buf
debug_print_crt mbedtls_debug_print_crt
debug_print_ecp mbedtls_debug_print_ecp
debug_print_mpi mbedtls_debug_print_mpi
debug_print_msg mbedtls_debug_print_msg
debug_print_ret mbedtls_debug_print_ret
debug_set_log_mode mbedtls_debug_set_log_mode
debug_set_threshold mbedtls_debug_set_threshold
des3_context mbedtls_des3_context
des3_crypt_cbc mbedtls_des3_crypt_cbc
des3_crypt_ecb mbedtls_des3_crypt_ecb
des3_free mbedtls_des3_free
des3_init
mbedtls_des3_init
des3_set2key_dec mbedtls_des3_set2key_dec
des3_set2key_enc mbedtls_des3_set2key_enc

des3_set3key_dec mbedtls_des3_set3key_dec
des3_set3key_enc mbedtls_des3_set3key_enc
des_context mbedtls_des_context
des_crypt_cbc mbedtls_des_crypt_cbc
des_crypt_ecb mbedtls_des_crypt_ecb
des_free mbedtls_des_free
des_init mbedtls_des_init
des_key_check_key_parity mbedtls_des_key_check_key_parity
des_key_check_weak mbedtls_des_key_check_weak
des_key_set_parity mbedtls_des_key_set_parity
des_self_test mbedtls_des_self_test
des_setkey_dec mbedtls_des_setkey_dec
des_setkey_enc mbedtls_des_setkey_enc
dhm_calc_secret mbedtls_dhm_calc_secret
dhm_context mbedtls_dhm_context
dhm_free mbedtls_dhm_free
dhm_init mbedtls_dhm_init
dhm_make_params mbedtls_dhm_make_params
dhm_make_public mbedtls_dhm_make_public
dhm_parse_dhm mbedtls_dhm_parse_dhm
dhm_parse_dhmfile mbedtls_dhm_parse_dhmfile
dhm_read_params mbedtls_dhm_read_params
dhm_read_public mbedtls_dhm_read_public
dhm_self_test mbedtls_dhm_self_test
ecdh_calc_secret
mbedtls_ecdh_calc_secret
ecdh_compute_shared mbedtls_ecdh_compute_shared
ecdh_context mbedtls_ecdh_context
ecdh_free mbedtls_ecdh_free
ecdh_gen_public mbedtls_ecdh_gen_public
ecdh_get_params mbedtls_ecdh_get_params
ecdh_init mbedtls_ecdh_init
ecdh_make_params mbedtls_ecdh_make_params
ecdh_make_public mbedtls_ecdh_make_public
ecdh_read_params mbedtls_ecdh_read_params
ecdh_read_public mbedtls_ecdh_read_public
ecdh_self_test mbedtls_ecdh_self_test
ecdh_side mbedtls_ecdh_side
ecdsa_context mbedtls_ecdsa_context
ecdsa_free mbedtls_ecdsa_free
ecdsa_from_keypair mbedtls_ecdsa_from_keypair
ecdsa_genkey mbedtls_ecdsa_genkey
ecdsa_info mbedtls_ecdsa_info
ecdsa_init mbedtls_ecdsa_init
ecdsa_read_signature mbedtls_ecdsa_read_signature
ecdsa_self_test mbedtls_ecdsa_self_test
ecdsa_sign mbedtls_ecdsa_sign
ecdsa_sign_det mbedtls_ecdsa_sign_det

ecdsa_verify mbedtls_ecdsa_verify
ecdsa_write_signature mbedtls_ecdsa_write_signature
ecdsa_write_signature_det mbedtls_ecdsa_write_signature_det
eckey_info
mbedtls_eckey_info
eckeydh_info mbedtls_eckeydh_info
ecp_add mbedtls_ecp_add
ecp_check_privkey mbedtls_ecp_check_privkey
ecp_check_pub_priv mbedtls_ecp_check_pub_priv
ecp_check_pubkey mbedtls_ecp_check_pubkey
ecp_copy mbedtls_ecp_copy
ecp_curve_info mbedtls_ecp_curve_info
ecp_curve_info_from_grp_id mbedtls_ecp_curve_info_from_grp_id
ecp_curve_info_from_name mbedtls_ecp_curve_info_from_name
ecp_curve_info_from_tls_id mbedtls_ecp_curve_info_from_tls_id
ecp_curve_list mbedtls_ecp_curve_list
ecp_gen_key mbedtls_ecp_gen_key
ecp_gen_keypair mbedtls_ecp_gen_keypair
ecp_group mbedtls_ecp_group
ecp_group_copy mbedtls_ecp_group_copy
ecp_group_free mbedtls_ecp_group_free
ecp_group_id mbedtls_ecp_group_id
ecp_group_init mbedtls_ecp_group_init
ecp_group_read_string mbedtls_ecp_group_read_string
ecp_grp_id_list mbedtls_ecp_grp_id_list
ecp_is_zero mbedtls_ecp_is_zero
ecp_keypair mbedtls_ecp_keypair
ecp_keypair_free mbedtls_ecp_keypair_free
ecp_keypair_init mbedtls_ecp_keypair_init
ecp_mul
mbedtls_ecp_mul
ecp_point mbedtls_ecp_point
ecp_point_free mbedtls_ecp_point_free
ecp_point_init mbedtls_ecp_point_init
ecp_point_read_binary mbedtls_ecp_point_read_binary
ecp_point_read_string mbedtls_ecp_point_read_string
ecp_point_write_binary mbedtls_ecp_point_write_binary
ecp_self_test mbedtls_ecp_self_test
ecp_set_zero mbedtls_ecp_set_zero
ecp_sub mbedtls_ecp_sub
ecp_tls_read_group mbedtls_ecp_tls_read_group
ecp_tls_read_point mbedtls_ecp_tls_read_point
ecp_tls_write_group mbedtls_ecp_tls_write_group
ecp_tls_write_point mbedtls_ecp_tls_write_point
ecp_use_known_dp mbedtls_ecp_group_load
entropy_add_source mbedtls_entropy_add_source
entropy_context mbedtls_entropy_context
entropy_free mbedtls_entropy_free

entropy_func mbedtls_entropy_func
entropy_gather mbedtls_entropy_gather
entropy_init mbedtls_entropy_init
entropy_self_test mbedtls_entropy_self_test
entropy_update_manual mbedtls_entropy_update_manual
entropy_update_seed_file mbedtls_entropy_update_seed_file
entropy_write_seed_file
mbedtls_entropy_write_seed_file
error_strerror mbedtls_strerror
f_source_ptr mbedtls_entropy_f_source_ptr
gcm_auth_decrypt mbedtls_gcm_auth_decrypt
gcm_context mbedtls_gcm_context
gcm_crypt_and_tag mbedtls_gcm_crypt_and_tag
gcm_finish mbedtls_gcm_finish
gcm_free mbedtls_gcm_free
gcm_init mbedtls_gcm_init
gcm_self_test mbedtls_gcm_self_test
gcm_starts mbedtls_gcm_starts
gcm_update mbedtls_gcm_update
get_timer mbedtls_timing_get_timer
hardclock mbedtls_timing_hardclock
hardclock_poll mbedtls_hardclock_poll
havege_free mbedtls_havege_free
havege_init mbedtls_havege_init
havege_poll mbedtls_havege_poll
havege_random mbedtls_havege_random
havege_state mbedtls_havege_state
hmac_drbg_context mbedtls_hmac_drbg_context
hmac_drbg_free mbedtls_hmac_drbg_free
hmac_drbg_init mbedtls_hmac_drbg_init
hmac_drbg_init_buf mbedtls_hmac_drbg_init_buf
hmac_drbg_random mbedtls_hmac_drbg_random
hmac_drbg_random_with_add mbedtls_hmac_drbg_random_with_add
hmac_drbg_reseed mbedtls_hmac_drbg_reseed
hmac_drbg_self_test
mbedtls_hmac_drbg_self_test
hmac_drbg_set_entropy_len mbedtls_hmac_drbg_set_entropy_len
hmac_drbg_set_prediction_resistance mbedtls_hmac_drbg_set_prediction_resistance
hmac_drbg_set_reseed_interval mbedtls_hmac_drbg_set_reseed_interval
hmac_drbg_update mbedtls_hmac_drbg_update
hmac_drbg_update_seed_file mbedtls_hmac_drbg_update_seed_file
hmac_drbg_write_seed_file mbedtls_hmac_drbg_write_seed_file
hr_time mbedtls_timing_hr_time
key_exchange_type_t mbedtls_key_exchange_type_t
m_sleep mbedtls_timing_m_sleep
md mbedtls_md
md2 mbedtls_md2
md2_context mbedtls_md2_context

md2_file mbedtls_md2_file
md2_finish mbedtls_md2_finish
md2_free mbedtls_md2_free
md2_hmac mbedtls_md2_hmac
md2_hmac_finish mbedtls_md2_hmac_finish
md2_hmac_reset mbedtls_md2_hmac_reset
md2_hmac_starts mbedtls_md2_hmac_starts
md2_hmac_update mbedtls_md2_hmac_update
md2_info mbedtls_md2_info
md2_init mbedtls_md2_init
md2_process mbedtls_md2_process
md2_self_test mbedtls_md2_self_test
md2_starts mbedtls_md2_starts
md2_update
mbedtls_md2_update
md4 mbedtls_md4
md4_context mbedtls_md4_context
md4_file mbedtls_md4_file
md4_finish mbedtls_md4_finish
md4_free mbedtls_md4_free
md4_hmac mbedtls_md4_hmac
md4_hmac_finish mbedtls_md4_hmac_finish
md4_hmac_reset mbedtls_md4_hmac_reset
md4_hmac_starts mbedtls_md4_hmac_starts
md4_hmac_update mbedtls_md4_hmac_update
md4_info mbedtls_md4_info
md4_init mbedtls_md4_init
md4_process mbedtls_md4_process
md4_self_test mbedtls_md4_self_test
md4_starts mbedtls_md4_starts
md4_update mbedtls_md4_update
md5 mbedtls_md5
md5_context mbedtls_md5_context
md5_file mbedtls_md5_file
md5_finish mbedtls_md5_finish
md5_free mbedtls_md5_free
md5_hmac mbedtls_md5_hmac
md5_hmac_finish mbedtls_md5_hmac_finish
md5_hmac_reset mbedtls_md5_hmac_reset
md5_hmac_starts mbedtls_md5_hmac_starts
md5_hmac_update mbedtls_md5_hmac_update
md5_info mbedtls_md5_info
md5_init mbedtls_md5_init
md5_process mbedtls_md5_process
md5_self_test mbedtls_md5_self_test
md5_starts mbedtls_md5_starts
md5_update

mbedtls_md5_update
md_context_t mbedtls_md_context_t
md_file mbedtls_md_file
md_finish mbedtls_md_finish
md_free mbedtls_md_free
md_free_ctx mbedtls_md_free_ctx
md_get_name mbedtls_md_get_name
md_get_size mbedtls_md_get_size
md_get_type mbedtls_md_get_type
md_hmac mbedtls_md_hmac
md_hmac_finish mbedtls_md_hmac_finish
md_hmac_reset mbedtls_md_hmac_reset
md_hmac_starts mbedtls_md_hmac_starts
md_hmac_update mbedtls_md_hmac_update
md_info_from_string mbedtls_md_info_from_string
md_info_from_type mbedtls_md_info_from_type
md_info_t mbedtls_md_info_t
md_init mbedtls_md_init
md_init_ctx mbedtls_md_init_ctx
md_list mbedtls_md_list
md_process mbedtls_md_process
md_starts mbedtls_md_starts
md_type_t mbedtls_md_type_t
md_update mbedtls_md_update
memory_buffer_alloc_cur_get mbedtls_memory_buffer_alloc_cur_get
memory_buffer_alloc_free mbedtls_memory_buffer_alloc_free
memory_buffer_alloc_init mbedtls_memory_buffer_alloc_init
memory_buffer_alloc_max_get mbedtls_memory_buffer_alloc_max_get
memory_buffer_alloc_max_reset
mbedtls_memory_buffer_alloc_max_reset
memory_buffer_alloc_self_test mbedtls_memory_buffer_alloc_self_test
memory_buffer_alloc_status mbedtls_memory_buffer_alloc_status
memory_buffer_alloc_verify mbedtls_memory_buffer_alloc_verify
memory_buffer_set_verify mbedtls_memory_buffer_set_verify
memory_set_own mbedtls_memory_set_own
mpi mbedtls_mpi
mpi_add_abs mbedtls_mpi_add_abs
mpi_add_int mbedtls_mpi_add_int
mpi_add_mpi mbedtls_mpi_add_mpi
mpi_cmp_abs mbedtls_mpi_cmp_abs
mpi_cmp_int mbedtls_mpi_cmp_int
mpi_cmp_mpi mbedtls_mpi_cmp_mpi
mpi_copy mbedtls_mpi_copy
mpi_div_int mbedtls_mpi_div_int
mpi_div_mpi mbedtls_mpi_div_mpi
mpi_exp_mod mbedtls_mpi_exp_mod
mpi_fill_random mbedtls_mpi_fill_random
mpi_free mbedtls_mpi_free

mpi_gcd mbedtls_mpi_gcd
mpi_gen_prime mbedtls_mpi_gen_prime
mpi_get_bit mbedtls_mpi_get_bit
mpi_grow mbedtls_mpi_grow
mpi_init mbedtls_mpi_init
mpi_inv_mod mbedtls_mpi_inv_mod
mpi_is_prime mbedtls_mpi_is_prime
mpi_lsb mbedtls_mpi_lsb
mpi_lset mbedtls_mpi_lset
mpi_mod_int
mbedtls_mpi_mod_int
mpi_mod_mpi mbedtls_mpi_mod_mpi
mpi_msb mbedtls_mpi_bitlen
mpi_mul_int mbedtls_mpi_mul_int
mpi_mul_mpi mbedtls_mpi_mul_mpi
mpi_read_binary mbedtls_mpi_read_binary
mpi_read_file mbedtls_mpi_read_file
mpi_read_string mbedtls_mpi_read_string
mpi_safe_cond_assign mbedtls_mpi_safe_cond_assign
mpi_safe_cond_swap mbedtls_mpi_safe_cond_swap
mpi_self_test mbedtls_mpi_self_test
mpi_set_bit mbedtls_mpi_set_bit
mpi_shift_l mbedtls_mpi_shift_l
mpi_shift_r mbedtls_mpi_shift_r
mpi_shrink mbedtls_mpi_shrink
mpi_size mbedtls_mpi_size
mpi_sub_abs mbedtls_mpi_sub_abs
mpi_sub_int mbedtls_mpi_sub_int
mpi_sub_mpi mbedtls_mpi_sub_mpi
mpi_swap mbedtls_mpi_swap
mpi_write_binary mbedtls_mpi_write_binary
mpi_write_file mbedtls_mpi_write_file
mpi_write_string mbedtls_mpi_write_string
net_accept mbedtls_net_accept
net_bind mbedtls_net_bind
net_close mbedtls_net_free
net_connect mbedtls_net_connect
net_recv mbedtls_net_recv
net_recv_timeout mbedtls_net_recv_timeout
net_send
mbedtls_net_send
net_set_block mbedtls_net_set_block
net_set_nonblock mbedtls_net_set_nonblock
net_usleep mbedtls_net_usleep
oid_descriptor_t mbedtls_oid_descriptor_t
oid_get_attr_short_name mbedtls_oid_get_attr_short_name
oid_get_cipher_alg mbedtls_oid_get_cipher_alg
oid_get_ec_grp mbedtls_oid_get_ec_grp

oid_get_extended_key_usage mbedtls_oid_get_extended_key_usage
oid_get_md_alg mbedtls_oid_get_md_alg
oid_get_numeric_string mbedtls_oid_get_numeric_string
oid_get_oid_by_ec_grp mbedtls_oid_get_oid_by_ec_grp
oid_get_oid_by_md mbedtls_oid_get_oid_by_md
oid_get_oid_by_pk_alg mbedtls_oid_get_oid_by_pk_alg
oid_get_oid_by_sig_alg mbedtls_oid_get_oid_by_sig_alg
oid_get_pk_alg mbedtls_oid_get_pk_alg
oid_get_pkcs12_pbe_alg mbedtls_oid_get_pkcs12_pbe_alg
oid_get_sig_alg mbedtls_oid_get_sig_alg
oid_get_sig_alg_desc mbedtls_oid_get_sig_alg_desc
oid_get_x509_ext_type mbedtls_oid_get_x509_ext_type
operation_t mbedtls_operation_t
padlock_supports mbedtls_padlock_has_support
padlock_xcryptcbc mbedtls_padlock_xcryptcbc
padlock_xcryptecb
mbedtls_padlock_xcryptecb
pem_context mbedtls_pem_context
pem_free mbedtls_pem_free
pem_init mbedtls_pem_init
pem_read_buffer mbedtls_pem_read_buffer
pem_write_buffer mbedtls_pem_write_buffer
pk_can_do mbedtls_pk_can_do
pk_check_pair mbedtls_pk_check_pair
pk_context mbedtls_pk_context
pk_debug mbedtls_pk_debug
pk_debug_item mbedtls_pk_debug_item
pk_debug_type mbedtls_pk_debug_type
pk_decrypt mbedtls_pk_decrypt
pk_ec mbedtls_pk_ec
pk_encrypt mbedtls_pk_encrypt
pk_free mbedtls_pk_free
pk_get_len mbedtls_pk_get_len
pk_get_name mbedtls_pk_get_name
pk_get_size mbedtls_pk_get_bitlen
pk_get_type mbedtls_pk_get_type
pk_info_from_type mbedtls_pk_info_from_type
pk_info_t mbedtls_pk_info_t
pk_init mbedtls_pk_init
pk_init_ctx mbedtls_pk_setup
pk_init_ctx_rsa_alt mbedtls_pk_setup_rsa_alt
pk_load_file mbedtls_pk_load_file
pk_parse_key mbedtls_pk_parse_key
pk_parse_keyfile mbedtls_pk_parse_keyfile
pk_parse_public_key mbedtls_pk_parse_public_key
pk_parse_public_keyfile
mbedtls_pk_parse_public_keyfile
pk_parse_subpubkey mbedtls_pk_parse_subpubkey

pk_rsa mbedtls_pk_rsa
pk_rsa_alt_decrypt_func mbedtls_pk_rsa_alt_decrypt_func
pk_rsa_alt_key_len_func mbedtls_pk_rsa_alt_key_len_func
pk_rsa_alt_sign_func mbedtls_pk_rsa_alt_sign_func
pk_rsassa_pss_options mbedtls_pk_rsassa_pss_options
pk_sign mbedtls_pk_sign
pk_type_t mbedtls_pk_type_t
pk_verify mbedtls_pk_verify
pk_verify_ext mbedtls_pk_verify_ext
pk_write_key_der mbedtls_pk_write_key_der
pk_write_key_pem mbedtls_pk_write_key_pem
pk_write_pubkey mbedtls_pk_write_pubkey
pk_write_pubkey_der mbedtls_pk_write_pubkey_der
pk_write_pubkey_pem mbedtls_pk_write_pubkey_pem
pkcs11_context mbedtls_pkcs11_context
pkcs11_decrypt mbedtls_pkcs11_decrypt
pkcs11_priv_key_free mbedtls_pkcs11_priv_key_free
pkcs11_priv_key_init mbedtls_pkcs11_priv_key_bind
pkcs11_sign mbedtls_pkcs11_sign
pkcs11_x509_cert_init mbedtls_pkcs11_x509_cert_bind
pkcs12_derivation mbedtls_pkcs12_derivation
pkcs12_pbe mbedtls_pkcs12_pbe
pkcs12_pbe_sha1_rc4_128
mbedtls_pkcs12_pbe_sha1_rc4_128
pkcs5_pbes2 mbedtls_pkcs5_pbes2
pkcs5_pbkdf2_hmac mbedtls_pkcs5_pbkdf2_hmac
pkcs5_self_test mbedtls_pkcs5_self_test
platform_entropy_poll mbedtls_platform_entropy_poll
platform_set_exit mbedtls_platform_set_exit
platform_set_fprintf mbedtls_platform_set_fprintf
platform_set_malloc_free mbedtls_platform_set_malloc_free
platform_set_printf mbedtls_platform_set_printf
platform_set_snprintf mbedtls_platform_set_snprintf
polarssl_exit mbedtls_exit
polarssl_fprintf mbedtls_fprintf
polarssl_free mbedtls_free
polarssl_malloc mbedtls_malloc
polarssl_mutex_free mbedtls_mutex_free
polarssl_mutex_init mbedtls_mutex_init
polarssl_mutex_lock mbedtls_mutex_lock
polarssl_mutex_unlock mbedtls_mutex_unlock
polarssl_printf mbedtls_printf
polarssl_snprintf mbedtls_snprintf
polarssl_strerror mbedtls_strerror
ripemd160 mbedtls_ripemd160
ripemd160_context mbedtls_ripemd160_context
ripemd160_file mbedtls_ripemd160_file
ripemd160_finish mbedtls_ripemd160_finish

ripemd160_free
mbedtls_ripemd160_free
ripemd160_hmac mbedtls_ripemd160_hmac
ripemd160_hmac_finish mbedtls_ripemd160_hmac_finish
ripemd160_hmac_reset mbedtls_ripemd160_hmac_reset
ripemd160_hmac_starts mbedtls_ripemd160_hmac_starts
ripemd160_hmac_update mbedtls_ripemd160_hmac_update
ripemd160_info mbedtls_ripemd160_info
ripemd160_init mbedtls_ripemd160_init
ripemd160_process mbedtls_ripemd160_process
ripemd160_self_test mbedtls_ripemd160_self_test
ripemd160_starts mbedtls_ripemd160_starts
ripemd160_update mbedtls_ripemd160_update
rsa_alt_context mbedtls_rsa_alt_context
rsa_alt_info mbedtls_rsa_alt_info
rsa_check_privkey mbedtls_rsa_check_privkey
rsa_check_pub_priv mbedtls_rsa_check_pub_priv
rsa_check_pubkey mbedtls_rsa_check_pubkey
rsa_context mbedtls_rsa_context
rsa_copy mbedtls_rsa_copy
rsa_decrypt_func mbedtls_rsa_decrypt_func
rsa_free mbedtls_rsa_free
rsa_gen_key mbedtls_rsa_gen_key
rsa_info mbedtls_rsa_info
rsa_init mbedtls_rsa_init
rsa_key_len_func mbedtls_rsa_key_len_func
rsa_pkcs1_decrypt
mbedtls_rsa_pkcs1_decrypt
rsa_pkcs1_encrypt mbedtls_rsa_pkcs1_encrypt
rsa_pkcs1_sign mbedtls_rsa_pkcs1_sign
rsa_pkcs1_verify mbedtls_rsa_pkcs1_verify
rsa_private mbedtls_rsa_private
rsa_public mbedtls_rsa_public
rsa_rsaes_oaep_decrypt mbedtls_rsa_rsaes_oaep_decrypt
rsa_rsaes_oaep_encrypt mbedtls_rsa_rsaes_oaep_encrypt
rsa_rsaes_pkcs1_v15_decrypt mbedtls_rsa_rsaes_pkcs1_v15_decrypt
rsa_rsaes_pkcs1_v15_encrypt mbedtls_rsa_rsaes_pkcs1_v15_encrypt
rsa_rsassa_pkcs1_v15_sign mbedtls_rsa_rsassa_pkcs1_v15_sign
rsa_rsassa_pkcs1_v15_verify mbedtls_rsa_rsassa_pkcs1_v15_verify
rsa_rsassa_pss_sign mbedtls_rsa_rsassa_pss_sign
rsa_rsassa_pss_verify mbedtls_rsa_rsassa_pss_verify
rsa_rsassa_pss_verify_ext mbedtls_rsa_rsassa_pss_verify_ext
rsa_self_test mbedtls_rsa_self_test
rsa_set_padding mbedtls_rsa_set_padding
rsa_sign_func mbedtls_rsa_sign_func
safer_memcmp mbedtls_ssl_safer_memcmp
set_alarm mbedtls_set_alarm
sha1 mbedtls_sha1

sha1_context mbedtls_sha1_context
sha1_file mbedtls_sha1_file
sha1_finish
mbedtls_sha1_finish
sha1_free mbedtls_sha1_free
sha1_hmac mbedtls_sha1_hmac
sha1_hmac_finish mbedtls_sha1_hmac_finish
sha1_hmac_reset mbedtls_sha1_hmac_reset
sha1_hmac_starts mbedtls_sha1_hmac_starts
sha1_hmac_update mbedtls_sha1_hmac_update
sha1_info mbedtls_sha1_info
sha1_init mbedtls_sha1_init
sha1_process mbedtls_sha1_process
sha1_self_test mbedtls_sha1_self_test
sha1_starts mbedtls_sha1_starts
sha1_update mbedtls_sha1_update
sha224_info mbedtls_sha224_info
sha256 mbedtls_sha256
sha256_context mbedtls_sha256_context
sha256_file mbedtls_sha256_file
sha256_finish mbedtls_sha256_finish
sha256_free mbedtls_sha256_free
sha256_hmac mbedtls_sha256_hmac
sha256_hmac_finish mbedtls_sha256_hmac_finish
sha256_hmac_reset mbedtls_sha256_hmac_reset
sha256_hmac_starts mbedtls_sha256_hmac_starts
sha256_hmac_update mbedtls_sha256_hmac_update
sha256_info mbedtls_sha256_info
sha256_init mbedtls_sha256_init
sha256_process mbedtls_sha256_process
sha256_self_test mbedtls_sha256_self_test
sha256_starts
mbedtls_sha256_starts
sha256_update mbedtls_sha256_update
sha384_info mbedtls_sha384_info
sha512 mbedtls_sha512
sha512_context mbedtls_sha512_context
sha512_file mbedtls_sha512_file
sha512_finish mbedtls_sha512_finish
sha512_free mbedtls_sha512_free
sha512_hmac mbedtls_sha512_hmac
sha512_hmac_finish mbedtls_sha512_hmac_finish
sha512_hmac_reset mbedtls_sha512_hmac_reset
sha512_hmac_starts mbedtls_sha512_hmac_starts
sha512_hmac_update mbedtls_sha512_hmac_update
sha512_info mbedtls_sha512_info
sha512_init mbedtls_sha512_init
sha512_process mbedtls_sha512_process

sha512_self_test mbedtls_sha512_self_test
sha512_starts mbedtls_sha512_starts
sha512_update mbedtls_sha512_update
source_state mbedtls_entropy_source_state
ssl_cache_context mbedtls_ssl_cache_context
ssl_cache_entry mbedtls_ssl_cache_entry
ssl_cache_free mbedtls_ssl_cache_free
ssl_cache_get mbedtls_ssl_cache_get
ssl_cache_init mbedtls_ssl_cache_init
ssl_cache_set mbedtls_ssl_cache_set
ssl_cache_set_max_entries mbedtls_ssl_cache_set_max_entries
ssl_cache_set_timeout
mbedtls_ssl_cache_set_timeout
ssl_check_cert_usage mbedtls_ssl_check_cert_usage
ssl_ciphersuite_from_id mbedtls_ssl_ciphersuite_from_id
ssl_ciphersuite_from_string mbedtls_ssl_ciphersuite_from_string
ssl_ciphersuite_t mbedtls_ssl_ciphersuite_t
ssl_ciphersuite_uses_ec mbedtls_ssl_ciphersuite_uses_ec
ssl_ciphersuite_uses_psk mbedtls_ssl_ciphersuite_uses_psk
ssl_close_notify mbedtls_ssl_close_notify
ssl_context mbedtls_ssl_context
ssl_cookie_check mbedtls_ssl_cookie_check
ssl_cookie_check_t mbedtls_ssl_cookie_check_t
ssl_cookie_ctx mbedtls_ssl_cookie_ctx
ssl_cookie_free mbedtls_ssl_cookie_free
ssl_cookie_init mbedtls_ssl_cookie_init
ssl_cookie_set_timeout mbedtls_ssl_cookie_set_timeout
ssl_cookie_setup mbedtls_ssl_cookie_setup
ssl_cookie_write mbedtls_ssl_cookie_write
ssl_cookie_write_t mbedtls_ssl_cookie_write_t
ssl_curve_is_acceptable mbedtls_ssl_curve_is_acceptable
ssl_derive_keys mbedtls_ssl_derive_keys
ssl_dtls_replay_check mbedtls_ssl_dtls_replay_check
ssl_dtls_replay_update
mbedtls_ssl_dtls_replay_update
ssl_fetch_input mbedtls_ssl_fetch_input
ssl_flight_item mbedtls_ssl_flight_item
ssl_flush_output mbedtls_ssl_flush_output
ssl_free mbedtls_ssl_free
ssl_get_alpn_protocol mbedtls_ssl_get_alpn_protocol
ssl_get_bytes_avail mbedtls_ssl_get_bytes_avail
ssl_get_ciphersuite mbedtls_ssl_get_ciphersuite
ssl_get_ciphersuite_id mbedtls_ssl_get_ciphersuite_id
ssl_get_ciphersuite_name mbedtls_ssl_get_ciphersuite_name
ssl_get_ciphersuite_sig_pk_alg mbedtls_ssl_get_ciphersuite_sig_pk_alg
ssl_get_peer_cert mbedtls_ssl_get_peer_cert
ssl_get_record_expansion mbedtls_ssl_get_record_expansion
ssl_get_session mbedtls_ssl_get_session

ssl_get_verify_result mbedtls_ssl_get_verify_result
ssl_get_version mbedtls_ssl_get_version
ssl_handshake mbedtls_ssl_handshake
ssl_handshake_client_step mbedtls_ssl_handshake_client_step
ssl_handshake_free mbedtls_ssl_handshake_free
ssl_handshake_params mbedtls_ssl_handshake_params
ssl_handshake_server_step
mbedtls_ssl_handshake_server_step
ssl_handshake_step mbedtls_ssl_handshake_step
ssl_handshake_wrapup mbedtls_ssl_handshake_wrapup
ssl_hdr_len mbedtls_ssl_hdr_len
ssl_hs_hdr_len mbedtls_ssl_hs_hdr_len
ssl_hw_record_activate mbedtls_ssl_hw_record_activate
ssl_hw_record_finish mbedtls_ssl_hw_record_finish
ssl_hw_record_init mbedtls_ssl_hw_record_init
ssl_hw_record_read mbedtls_ssl_hw_record_read
ssl_hw_record_reset mbedtls_ssl_hw_record_reset
ssl_hw_record_write mbedtls_ssl_hw_record_write
ssl_init mbedtls_ssl_init
ssl_key_cert mbedtls_ssl_key_cert
ssl_legacy_renegotiation mbedtls_ssl_conf_legacy_renegotiation
ssl_list_ciphersuites mbedtls_ssl_list_ciphersuites
ssl_md_alg_from_hash mbedtls_ssl_md_alg_from_hash
ssl_optimize_checksum mbedtls_ssl_optimize_checksum
ssl_own_cert mbedtls_ssl_own_cert
ssl_own_key mbedtls_ssl_own_key
ssl_parse_certificate mbedtls_ssl_parse_certificate
ssl_parse_change_cipher_spec mbedtls_ssl_parse_change_cipher_spec
ssl_parse_finished mbedtls_ssl_parse_finished
ssl_pk_alg_from_sig
mbedtls_ssl_pk_alg_from_sig
ssl_pkcs11_decrypt mbedtls_ssl_pkcs11_decrypt
ssl_pkcs11_key_len mbedtls_ssl_pkcs11_key_len
ssl_pkcs11_sign mbedtls_ssl_pkcs11_sign
ssl_psk_derive_premaster mbedtls_ssl_psk_derive_premaster
ssl_read mbedtls_ssl_read
ssl_read_record mbedtls_ssl_read_record
ssl_read_version mbedtls_ssl_read_version
ssl_recv_flight_completed mbedtls_ssl_recv_flight_completed
ssl_renegotiate mbedtls_ssl_renegotiate
ssl_resend mbedtls_ssl_resend
ssl_reset_checksum mbedtls_ssl_reset_checksum
ssl_send_alert_message mbedtls_ssl_send_alert_message
ssl_send_fatal_handshake_failure mbedtls_ssl_send_fatal_handshake_failure
ssl_send_flight_completed mbedtls_ssl_send_flight_completed
ssl_session mbedtls_ssl_session
ssl_session_free mbedtls_ssl_session_free
ssl_session_init mbedtls_ssl_session_init

ssl_session_reset mbedtls_ssl_session_reset
ssl_set_alpn_protocols mbedtls_ssl_conf_alpn_protocols
ssl_set_arc4_support mbedtls_ssl_conf_arc4_support
ssl_set_authmode mbedtls_ssl_conf_authmode
ssl_set_bio
mbedtls_ssl_set_bio
ssl_set_ca_chain mbedtls_ssl_conf_ca_chain
ssl_set_cbc_record_splitting mbedtls_ssl_conf_cbc_record_splitting
ssl_set_ciphersuites mbedtls_ssl_conf_ciphersuites
ssl_set_ciphersuites_for_version mbedtls_ssl_conf_ciphersuites_for_version
ssl_set_client_transport_id mbedtls_ssl_set_client_transport_id
ssl_set_curves mbedtls_ssl_conf_curves
ssl_set_dbg mbedtls_ssl_conf_dbg
ssl_set_dh_param mbedtls_ssl_conf_dh_param
ssl_set_dh_param_ctx mbedtls_ssl_conf_dh_param_ctx
ssl_set_dtls_anti_replay mbedtls_ssl_conf_dtls_anti_replay
ssl_set_dtls_badmac_limit mbedtls_ssl_conf_dtls_badmac_limit
ssl_set_dtls_cookies mbedtls_ssl_conf_dtls_cookies
ssl_set_encrypt_then_mac mbedtls_ssl_conf_encrypt_then_mac
ssl_set_endpoint mbedtls_ssl_conf_endpoint
ssl_set_extended_master_secret mbedtls_ssl_conf_extended_master_secret
ssl_set_fallback mbedtls_ssl_conf_fallback
ssl_set_handshake_timeout mbedtls_ssl_conf_handshake_timeout
ssl_set_hostname mbedtls_ssl_set_hostname
ssl_set_max_frag_len
mbedtls_ssl_conf_max_frag_len
ssl_set_max_version mbedtls_ssl_conf_max_version
ssl_set_min_version mbedtls_ssl_conf_min_version
ssl_set_own_cert mbedtls_ssl_conf_own_cert
ssl_set_own_cert_alt mbedtls_ssl_set_own_cert_alt
ssl_set_own_cert_rsa mbedtls_ssl_set_own_cert_rsa
ssl_set_psk mbedtls_ssl_conf_psk
ssl_set_psk_cb mbedtls_ssl_conf_psk_cb
ssl_set_renegotiation mbedtls_ssl_conf_renegotiation
ssl_set_renegotiation_enforced mbedtls_ssl_conf_renegotiation_enforced
ssl_set_renegotiation_period mbedtls_ssl_conf_renegotiation_period
ssl_set_rng mbedtls_ssl_conf_rng
ssl_set_session mbedtls_ssl_set_session
ssl_set_session_cache mbedtls_ssl_conf_session_cache
ssl_set_session_ticket_lifetime mbedtls_ssl_conf_session_ticket_lifetime
ssl_set_session_tickets mbedtls_ssl_conf_session_tickets
ssl_set_sni mbedtls_ssl_conf_sni
ssl_set_transport mbedtls_ssl_conf_transport
ssl_set_truncated_hmac mbedtls_ssl_conf_truncated_hmac
ssl_set_verify mbedtls_ssl_conf_verify
ssl_sig_from_pk
mbedtls_ssl_sig_from_pk
ssl_states mbedtls_ssl_states

ssl_ticket_keys mbedtls_ssl_ticket_keys
ssl_transform mbedtls_ssl_transform
ssl_transform_free mbedtls_ssl_transform_free
ssl_write mbedtls_ssl_write
ssl_write_certificate mbedtls_ssl_write_certificate
ssl_write_change_cipher_spec mbedtls_ssl_write_change_cipher_spec
ssl_write_finished mbedtls_ssl_write_finished
ssl_write_record mbedtls_ssl_write_record
ssl_write_version mbedtls_ssl_write_version
supported_ciphers mbedtls_cipher_supported
t_sint mbedtls_mpi_sint
t_udbl mbedtls_t_udbl
t_uint mbedtls_mpi_uint
test_ca_crt mbedtls_test_ca_crt
test_ca_crt_ec mbedtls_test_ca_crt_ec
test_ca_crt_rsa mbedtls_test_ca_crt_rsa
test_ca_key mbedtls_test_ca_key
test_ca_key_ec mbedtls_test_ca_key_ec
test_ca_key_rsa mbedtls_test_ca_key_rsa
test_ca_list mbedtls_test_cas_pem
test_ca_pwd mbedtls_test_ca_pwd
test_ca_pwd_ec mbedtls_test_ca_pwd_ec
test_ca_pwd_rsa mbedtls_test_ca_pwd_rsa
test_cli_crt mbedtls_test_cli_crt
test_cli_crt_ec mbedtls_test_cli_crt_ec
test_cli_crt_rsa
mbedtls_test_cli_crt_rsa
test_cli_key mbedtls_test_cli_key
test_cli_key_ec mbedtls_test_cli_key_ec
test_cli_key_rsa mbedtls_test_cli_key_rsa
test_dhm_params mbedtls_test_dhm_params
test_srv_crt mbedtls_test_srv_crt
test_srv_crt_ec mbedtls_test_srv_crt_ec
test_srv_crt_rsa mbedtls_test_srv_crt_rsa
test_srv_key mbedtls_test_srv_key
test_srv_key_ec mbedtls_test_srv_key_ec
test_srv_key_rsa mbedtls_test_srv_key_rsa
threading_mutex_t mbedtls_threading_mutex_t
threading_set_alt mbedtls_threading_set_alt
timing_self_test mbedtls_timing_self_test
version_check_feature mbedtls_version_check_feature
version_get_number mbedtls_version_get_number
version_get_string mbedtls_version_get_string
version_get_string_full mbedtls_version_get_string_full
x509_bitstring mbedtls_x509_bitstring
x509_buf mbedtls_x509_buf
x509_crl mbedtls_x509_crl
x509_crl_entry mbedtls_x509_crl_entry

x509_crl_free mbedtls_x509_crl_free
x509_crl_info mbedtls_x509_crl_info
x509_crl_init mbedtls_x509_crl_init
x509_crl_parse
mbedtls_x509_crl_parse
x509_crl_parse_der mbedtls_x509_crl_parse_der
x509_crl_parse_file mbedtls_x509_crl_parse_file
x509_crt mbedtls_x509_crt
x509_crt_check_extended_key_usage mbedtls_x509_crt_check_extended_key_usage
x509_crt_check_key_usage mbedtls_x509_crt_check_key_usage
x509_crt_free mbedtls_x509_crt_free
x509_crt_info mbedtls_x509_crt_info
x509_crt_init mbedtls_x509_crt_init
x509_crt_parse mbedtls_x509_crt_parse
x509_crt_parse_der mbedtls_x509_crt_parse_der
x509_crt_parse_file mbedtls_x509_crt_parse_file
x509_crt_parse_path mbedtls_x509_crt_parse_path
x509_crt_revoked mbedtls_x509_crt_is_revoked
x509_crt_verify mbedtls_x509_crt_verify
x509_crt_verify_info mbedtls_x509_crt_verify_info
x509_csr mbedtls_x509_csr
x509_csr_free mbedtls_x509_csr_free
x509_csr_info mbedtls_x509_csr_info
x509_csr_init mbedtls_x509_csr_init
x509_csr_parse mbedtls_x509_csr_parse
x509_csr_parse_der mbedtls_x509_csr_parse_der
x509_csr_parse_file mbedtls_x509_csr_parse_file
x509_dn_gets
mbedtls_x509_dn_gets
x509_get_alg mbedtls_x509_get_alg
x509_get_alg_null mbedtls_x509_get_alg_null
x509_get_ext mbedtls_x509_get_ext
x509_get_name mbedtls_x509_get_name
x509_get_rsassa_pss_params mbedtls_x509_get_rsassa_pss_params
x509_get_serial mbedtls_x509_get_serial
x509_get_sig mbedtls_x509_get_sig
x509_get_sig_alg mbedtls_x509_get_sig_alg
x509_get_time mbedtls_x509_get_time
x509_key_size_helper mbedtls_x509_key_size_helper
x509_name mbedtls_x509_name
x509_oid_get_description mbedtls_x509_oid_get_description
x509_oid_get_numeric_string mbedtls_x509_oid_get_numeric_string
x509_self_test mbedtls_x509_self_test
x509_sequence mbedtls_x509_sequence
x509_serial_gets mbedtls_x509_serial_gets
x509_set_extension mbedtls_x509_set_extension
x509_sig_alg_gets mbedtls_x509_sig_alg_gets
x509_string_to_names mbedtls_x509_string_to_names

x509_time mbedtls_x509_time
x509_time_expired mbedtls_x509_time_is_past
x509_time_future mbedtls_x509_time_is_future
x509_write_extensions mbedtls_x509_write_extensions
x509_write_names
mbedtls_x509_write_names
x509_write_sig mbedtls_x509_write_sig
x509write_cert mbedtls_x509write_cert
x509write_crt_der mbedtls_x509write_crt_der
x509write_crt_free mbedtls_x509write_crt_free
x509write_crt_init mbedtls_x509write_crt_init
x509write_crt_pem mbedtls_x509write_crt_pem
x509write_crt_set_authority_key_identifier mbedtls_x509write_crt_set_authority_key_identifier
x509write_crt_set_basic_constraints mbedtls_x509write_crt_set_basic_constraints
x509write_crt_set_extension mbedtls_x509write_crt_set_extension
x509write_crt_set_issuer_key mbedtls_x509write_crt_set_issuer_key
x509write_crt_set_issuer_name mbedtls_x509write_crt_set_issuer_name
x509write_crt_set_key_usage mbedtls_x509write_crt_set_key_usage
x509write_crt_set_md_alg mbedtls_x509write_crt_set_md_alg
x509write_crt_set_ns_cert_type mbedtls_x509write_crt_set_ns_cert_type
x509write_crt_set_serial mbedtls_x509write_crt_set_serial
x509write_crt_set_subject_key mbedtls_x509write_crt_set_subject_key
x509write_crt_set_subject_key_identifier
mbedtls_x509write_crt_set_subject_key_identifier
x509write_crt_set_subject_name mbedtls_x509write_crt_set_subject_name
x509write_crt_set_validity mbedtls_x509write_crt_set_validity
x509write_crt_set_version mbedtls_x509write_crt_set_version
x509write_csr mbedtls_x509write_csr
x509write_csr_der mbedtls_x509write_csr_der
x509write_csr_free mbedtls_x509write_csr_free
x509write_csr_init mbedtls_x509write_csr_init
x509write_csr_pem mbedtls_x509write_csr_pem
x509write_csr_set_extension mbedtls_x509write_csr_set_extension
x509write_csr_set_key mbedtls_x509write_csr_set_key
x509write_csr_set_key_usage mbedtls_x509write_csr_set_key_usage
x509write_csr_set_md_alg mbedtls_x509write_csr_set_md_alg
x509write_csr_set_ns_cert_type mbedtls_x509write_csr_set_ns_cert_type
x509write_csr_set_subject_name mbedtls_x509write_csr_set_subject_name
xtea_context mbedtls_xtea_context
xtea_crypt_cbc mbedtls_xtea_crypt_cbc
xtea_crypt_ecb mbedtls_xtea_crypt_ecb
xtea_free mbedtls_xtea_free
xtea_init
mbedtls_xtea_init
xtea_self_test mbedtls_xtea_self_test
xtea_setup mbedtls_xtea_setup
-----BEGIN CERTIFICATE-----
MIIDwjCCAaqgAwIBAgIBEDANBgkqhkiG9w0BAQsFADBIMQswCQYDVQQGEwJOTDER

MA8GA1UEChMIUG9sYXJTU0wxJjAkBgNVBAMTHVBvbGFyU1NMIFRlc3QgSW50ZXJt
ZWRpYXRlIENBMB4XDTEzMDkyNDE2MTIyNFoXDTIzMDkyMjE2MTIyNFowNDELMAk G
A1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NMMRIwEAYDVQQDEwlsb2NhbGhvc3Qw
WTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQcbffp2qXqoZyychmoCRxzrd4Vu96m
47NPBehtEC46aTeXgDnBdf++znABrAtfXBRNQz8ARIeYBmskr22rlKjyo4GVMIGS
MAkGA1UdEwQCMAAwHQYDVR0OBBYEFNIK06V3H85VsFxGoo5zbL+hYCa7MGYGA1Ud
IwRfMF2AFDh32Gt3nCh3gotO2BupHveUFrcOoUKkQDA+MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0GC
AQ4wDQYJKoZIhvcNAQELBQADggIBADRoQ5fHKw+vkl0D3aqLX1XrZidb+25AWbhr
FYXdaskN219PrXBL3cV8x5tK6qsPKSyyw1lue80OmhXs/w7PJkOHHUSWRnmTv7lr
8Us3Zr/yOF/VVqzdGs7DlOTpyzEBdugI9uar/aCqHDoltN8wOduOoQB9aojYpROj
+gjlEO0mgt/87XpjYOig1o0jv44QYDQZQzpj1zeIn6WMe6xk9YDwCLMjRIpg++c7
QyxvcEJTn80wX1SaEBM2gau97G7bORLMwBVkMT4oSY+iKYgpPpawOnMJbqUP73Dm
yfJExDdrW/BbWZ/vKIcSqSZIbkHdkNjUDVHczyVwQxZxzvLFw/B1k9s7jYFsi5eK
TNAdXFa4et1H2sd+uhu24GxsjmJioDrftixcgzPVBjDCjH8QWkBEX292WJ58on0e
deWLpZUnzPdE1B4rsiPw1Vg28mGgr2O1xgBQr/fx6A+8ItNTzAXbZfEcult9ypwM
0b6YDNe5IvdKk8iwz3mof0VNy47K6xoCaE/fxxWkjoXK8x2wfswGeP2QgUzQE93b
OtjdHpsG1c7gIVFQmKATyAPUz4vqmezgNRleXU0oL0PYtoCmKQ51UjNMUfmO9xCj
VJaNa2iTQ5Dgic+CW4TYAgj5/9g9X3WfwnDNxrZ0UxxawGElczHXqbrNleTtPaKp
a8Si6UK5
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEATCCA4egAwIBAgIBDjAKBggqhkjOPQQDAjA+MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EwHhcN
MTMwOTI0MTU1NTE0WhcNMjMwOTIyMTU1NTE0WjBIMQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxJjAkBgNVBAMTHVBvbGFyU1NMIFRlc3QgSW50ZXJtZWRp
YXRlIENBMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAo1Oc8nr6fMTq
vowV+CpC55i5BZGFGc50Eb4RLBSRTH1e7JepdFjAVbBtyQRJSiY1ja0tgLQDDKZR
wfEI+b4azse460InPHv7C1TN0upXlxuj6m9B1IlP+sBaM7WBC6dVfPO+jVMIxgkF
CaBCLhhdK1Fjf8HjkT/PkctWnho8NTwivc9+nqRZjXe/eIcqm5HwjDDhu+gz+o0g
Vz9MfZNi1JyCrOyNZcy+cr2QeNnNVGnFq8xTxtu6dLunhpmLFj2mm0Vjwa7Ypj5q
AjpqTMtDvqbRuToyoyzajhMNcCAf7gwzIupJJFVdjdtgYAcQwzikwF5HoITJzzJ2
qgxF7CmvGZNb7G99mLdLdhtclH3wAQKHYwEGJo7XKyNEuHPQgB+e0cg1SD1HqlAM
uCfGGTWQ6me7Bjan3t0NzoTdDq6IpKTesbaY+/9e2xn8DCrhBKLXQMZFDZqUoLYA
kGPOEGgvlPnIIXAawouxCaNYEh5Uw871YMSPT28rLdFr49dwYOtDg9foA8hDIW2P
d6KXbrZteesvA1nYzEOs+3AjrbT79Md2W8Bz9bqBVNlNOESSqm4kiCJFmslm/6br
Np0MSQd+o22PQ4xRtmP6UsTfU0ueiMpYc8TYYhMbfnfFyo4m707ebcflPbBEN2dg
updQ66cvfCJB0QJt9upafY0lpdV1qUkCAwEAAaOBoDCBnTAdBgNVHQ4EFgQUOHf
Y
a3ecKHeCi07YG6ke95QWtw4wbgYDVR0jBGcwZYAUnW0gJEkBPyvLeLUZvH4kydv7
NnyhQqRAMD4xCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UE
AxMTUG9sYXJzc2wgVGVzdCBFQyBDQYIJAMFD4n5iQ8zoMAwGA1UdEwQFMAMBAf8w
CgYIKoZIzj0EAwIDaAAwZQIxAPyE+u+eP7gRrSFjQicmpYg8jiFUCYEowWY2zuOG
i1HXYwmpDHfasQ3rNSuf/gHvjwIwbSSjumDk+uYNci/KMELDsD0MFHxZhhBc9Hp9
Af5cNR8KhzegznL6amRObGGKmX1F
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIICHjCCAaWgAwIBAgIBHTAKBggqhkjOPQQDAjA+MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EwHhcN
MzIwMzEwMTEwNDExWhcNNDIwMzA4MTEwNDExWjA0MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxEjAQBgNVBAMTCWxvY2FsaG9zdDBZMBMGByqGSM49AgEG
CCqGSM49AwEHA0IABDfMVtl2CR5acj7HWS3/IG7ufPkGkXTQrRS192giWWKSTuUA
2CMR/+ov0jRdXRa9iojCa3cNVc2KKg76Aci07f+jgZ0wgZowCQYDVR0TBAIwADAd
BgNVHQ4EFgQUUGlj9QH2deCAQzlZX+MY0anE74wbgYDVR0jBGcwZYAUnW0gJEkB
PyvLeLUZvH4kydv7NnyhQqRAMD4xCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQb2xh
clNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBFQyBDQYIJAMFD4n5iQ8zoMAoG
CCqGSM49BAMCA2cAMGQCMAZWcb+NYxFVK+W6Z5eknM2TrbqQGZEYHQXeV9/XF0t7
TLDhA6a/pFDTJVZunFzesgIwfqkBYuvMkiNlS4lWcVyf8L4CZIHCn1yHnOCxu8ix
uqgLb4na3i94x9urgbZZYfVK
-----END CERTIFICATE-----
NULL Encrypt and decrypt 0 bytes
depends_on:MBEDTLS_CIPHER_NULL_CIPHER
enc_dec_buf:MBEDTLS_CIPHER_NULL:"NULL":0:0:-1

NULL Encrypt and decrypt 1 bytes
depends_on:MBEDTLS_CIPHER_NULL_CIPHER
enc_dec_buf:MBEDTLS_CIPHER_NULL:"NULL":0:1:-1

NULL Encrypt and decrypt 2 bytes
depends_on:MBEDTLS_CIPHER_NULL_CIPHER
enc_dec_buf:MBEDTLS_CIPHER_NULL:"NULL":0:2:-1

NULL Encrypt and decrypt 7 bytes
depends_on:MBEDTLS_CIPHER_NULL_CIPHER
enc_dec_buf:MBEDTLS_CIPHER_NULL:"NULL":0:7:-1

NULL Encrypt and decrypt 8 bytes
depends_on:MBEDTLS_CIPHER_NULL_CIPHER
enc_dec_buf:MBEDTLS_CIPHER_NULL:"NULL":0:8:-1

NULL Encrypt and decrypt 9 bytes
depends_on:MBEDTLS_CIPHER_NULL_CIPHER
enc_dec_buf:MBEDTLS_CIPHER_NULL:"NULL":0:9:-1

NULL Encrypt and decrypt 15 bytes
depends_on:MBEDTLS_CIPHER_NULL_CIPHER
enc_dec_buf:MBEDTLS_CIPHER_NULL:"NULL":0:15:-1

NULL Encrypt and decrypt 16 bytes
depends_on:MBEDTLS_CIPHER_NULL_CIPHER
enc_dec_buf:MBEDTLS_CIPHER_NULL:"NULL":0:16:-1

NULL Encrypt and decrypt 31 bytes
depends_on:MBEDTLS_CIPHER_NULL_CIPHER

enc_dec_buf:MBEDTLS_CIPHER_NULL:"NULL":0:31:-1

NULL
Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_CIPHER_NULL_CIPHER
enc_dec_buf:MBEDTLS_CIPHER_NULL:"NULL":0:32:-1

NULL Encrypt and decrypt 33 bytes
depends_on:MBEDTLS_CIPHER_NULL_CIPHER
enc_dec_buf:MBEDTLS_CIPHER_NULL:"NULL":0:33:-1

NULL Encrypt and decrypt 47 bytes
depends_on:MBEDTLS_CIPHER_NULL_CIPHER
enc_dec_buf:MBEDTLS_CIPHER_NULL:"NULL":0:47:-1

NULL Encrypt and decrypt 48 bytes
depends_on:MBEDTLS_CIPHER_NULL_CIPHER
enc_dec_buf:MBEDTLS_CIPHER_NULL:"NULL":0:48:-1

NULL Encrypt and decrypt 49 bytes
depends_on:MBEDTLS_CIPHER_NULL_CIPHER
enc_dec_buf:MBEDTLS_CIPHER_NULL:"NULL":0:49:-1

NULL Encrypt and decrypt 1 bytes in multiple parts 1
depends_on:MBEDTLS_CIPHER_NULL_CIPHER
enc_dec_buf_multipart:MBEDTLS_CIPHER_NULL:0:1:0:

NULL Encrypt and decrypt 1 bytes in multiple parts 2
depends_on:MBEDTLS_CIPHER_NULL_CIPHER
enc_dec_buf_multipart:MBEDTLS_CIPHER_NULL:0:0:1:

NULL Encrypt and decrypt 16 bytes in multiple parts
1
depends_on:MBEDTLS_CIPHER_NULL_CIPHER
enc_dec_buf_multipart:MBEDTLS_CIPHER_NULL:0:16:0:

NULL Encrypt and decrypt 16 bytes in multiple parts 2
depends_on:MBEDTLS_CIPHER_NULL_CIPHER
enc_dec_buf_multipart:MBEDTLS_CIPHER_NULL:0:0:16:

NULL Encrypt and decrypt 16 bytes in multiple parts 3
depends_on:MBEDTLS_CIPHER_NULL_CIPHER
enc_dec_buf_multipart:MBEDTLS_CIPHER_NULL:0:1:15:

NULL Encrypt and decrypt 16 bytes in multiple parts 4
depends_on:MBEDTLS_CIPHER_NULL_CIPHER
enc_dec_buf_multipart:MBEDTLS_CIPHER_NULL:0:15:1:

NULL Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_CIPHER_NULL_CIPHER
enc_dec_buf_multipart:MBEDTLS_CIPHER_NULL:0:15:7:

NULL Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_CIPHER_NULL_CIPHER
enc_dec_buf_multipart:MBEDTLS_CIPHER_NULL:0:16:6:

NULL Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_CIPHER_NULL_CIPHER
enc_dec_buf_multipart:MBEDTLS_CIPHER_NULL:0:17:6:

NULL Encrypt and decrypt 32 bytes in multiple parts
1
depends_on:MBEDTLS_CIPHER_NULL_CIPHER
enc_dec_buf_multipart:MBEDTLS_CIPHER_NULL:0:16:16:
-----BEGIN PUBLIC KEY-----
MHowFAYHKoZIzj0CAQYJKyQDAwIIAQELA2IABHGfnQk6Yn4NNQOFxmHOvwDGGSNW
b+kAajEHrx2HG8a7aJhf1yLqMr4xb454O3zRlXeF9mz8DLGV3VyZqOerqoSFU6WE
39K0jnbURf4A3YvlkJbYd9RpbSO0vI2xRyTmag==
-----END PUBLIC KEY-----
-----BEGIN CERTIFICATE-----
MIIDFzCCAf+gAwIBAgIBATANBgkqhkiG9w0BAQsFADAmMSQwIgYDVQQDExtUZXN0
IGludGVybWVkaWF0ZSBtYXhwYXRoIDEwHhcNMDEwMTAxMDAwMDAwWhcNMzAxMjMx
MjM1OTU5WjAmMSQwIgYDVQQDExtUZXN0IGludGVybWVkaWF0ZSBtYXhwYXRoIDIw
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCs0qdKXytu/GTKpa2H0CE3
OPSIMM2hiYbavzUroyL+hFv9XVoxh5CGnVUxK7B9ifVvzyElrcV7tjuIlGwp1hLH
tx/YU22xksI/n5/NS/qrxkK5xjwEWB9lx93rwLK0QnfjYRZrir7yySoBKi6IlHOv
GOwl0V/JAslMWwUZlFmvYvoCWSWGrDAkxWVnHq+HoZ7YoM/bdJdsIIJYe3tt7L8D
cJVP5dQ8jSs8/Ehm8BbG339r3B7v/KdK8zuoMig9ag/YOu9jOb0QvYC2HdZoL4WV
N+7aasTQmDGWGOt7fk7AEl0EI8lDvr2O/5q6ad9jRCkxyq3lJwRy+M3MdVKgA1On
AgMBAAGjUDBOMAwGA1UdEwQFMAMBAQEwHQYDVR0OBBYEFM6u5GkjkxB8PDdQIGKD
D8t1Zv/9MB8GA1UdIwQYMBaAFMsPD4cvxQL4nxkPhuh1pDIls8qlMA0GCSqGSIb3
DQEBCwUAA4IBAQCLpKATt01DUM8wCiDFVSpmpiCBqxnLRfQuY+ta1p+f15LME+cT
94lwaYCfCBtXQYwiuVFYdK8ztWEStPg6BecMLPB2K9gO/talxUoVDumsmR83p+2y
8YJmFHyjr+BShsjP9paCjUQkJiMOiWRpNFNpScv0IOHmb8NLER3vX/tCmxyVHPg/
7tBpDXRD6jOyajYH4KUx6wddcYWb63N9sApVpRHNaqpUKjuiQwfUFZjA7AyK/FUS
/cO3++uq+CkZhBu8vupaznXD4h0E28GbZgvu/F0edB7f0Q5DpnuDJ6HFMYl3A2mM
m8pqKNnRYGCtQwppBYVsoBisga2ymtNud7K+
-----END
CERTIFICATE-----
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
<ItemGroup Label="ProjectConfigurations">
<ProjectConfiguration Include="Debug|Win32">
<Configuration>Debug</Configuration>
<Platform>Win32</Platform>

```
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
    <Configuration>Debug</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
    <Configuration>Release</Configuration>
    <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
    <Configuration>Release</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
</ItemGroup>
<ItemGroup>
  <ClCompile Include="..\..\programs\pkey\rsa_decrypt.c" />
</ItemGroup>
<ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">
    <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
</ItemGroup>
<PropertyGroup Label="Globals">
  <ProjectGuid>{E0D71D72-8DF4-CCFC-EF60-741EADAB8BF9}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>rsa_decrypt</RootNamespace>
</PropertyGroup>
<Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
```

```
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
 />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
   <PrecompiledHeader>
   </PrecompiledHeader>
   <WarningLevel>Level3</WarningLevel>
   <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
```

```
    <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
```

```
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
  </Link>
 </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
 <Import
 Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqQIfPUBq1VVTi/027oJl
LhVhXom/uOhFkNvuiBZS0/FDUEeWEllkh2v9K+BG+XO+3c+S4ZFb7Wagb4kpeUWA
0INq1UFDd185fAkER4KwVzlw7aPsFRkeqDMIR8EFQqn9TMO0390GH00QUUBncxMP
QPhtgSVfCrFTxjB+FTms+Vruf5KepgVb5xOXhbUjktnUJAbVCSWJdQfdphqPPwkZ
vq1lLGTrlZvc/kFeF6babFtpzAK6FCwWJJxK3M3Q91Jnc/EtoCP9fvQxyi1wyokL
BNsupk9wbp7OvViJ4lNZnm5akmXiiD8MlBmj3eXonZUT7Snbq3AS3FrKaxerUoJU
sQIDAQAB
-----END PUBLIC KEY-----
-----BEGIN CERTIFICATE REQUEST-----
MIIBGDCBvwIBADA0MQswCQYDVQQGEwJOTDERMA8GA1UEChMIUG9sYXJTU0wxEjAQ
BgNVBAMTCWxvY2FsaG9zdDBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABDfMVtl2
```

```
CR5acj7HWS3/IG7ufPkGkXTQrRS192giWWKSTuUA2CMR/+ov0jRdXRa9iojCa3cN
Vc2KKg76Aci07f+gKTAnBgkqhkiG9w0BCQ4xGjAYMAkGA1UdEwQCMAAwCwYDVR0P
BAQDAgXgMAoGCCqGSM49BAMBA0gAMEUCIDYaN1m9MRk5mhX1U8aZKd0alyGKWqcR
oglF2MsIii/2AiEAjFHs8XQ0Q4yDF8oLztCxlq3nAvqmPdQz9T+TkEfh+PA=
-----END CERTIFICATE REQUEST-----
-----BEGIN EC PRIVATE KEY-----
MIGkAgEBBDCD2RUOoHHwVxAzozi4hsGmEV1ttAPhKXZF14dvI6tEIOpke4WxdueF
lap01tGkXuqgBwYFK4EEACKhZANiAATD2is0QTdYL4dW/vyJuilDS07gbsMOV1Mz
OVjUUrSRlTkLI99fFyRiSPwalSnOLC2HwohSgK/Waqsh3bjTHG5YuMrosmmO80Gt
KcO0X3WnR2/VGSlVaZpTOyC0ZhZgMx4=
-----END EC PRIVATE KEY-----
-----BEGIN EC PRIVATE KEY-----
MHgCAQEEICFh1vLbdlJvpiwW81aoDwHzL3dnhLNqqZeZqLdmIID/oAsGCSskAwMC
CAEBB6FEA0IABHaMjK5KvKYwbbDtgbDEpiFcN4Bm7G1hbBRuE/HH34CblqtpEcJ9
igIznwkmhA5VI209HvviZp0JDkxMZg+tqR0=
-----END EC PRIVATE KEY-----
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 0 (0x0)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=NL, O=PolarSSL, CN=PolarSSL Test CA
    Validity
      Not Before: Feb 12 14:44:00 2011 GMT
      Not After : Feb 12 14:44:00 2021 GMT
    Subject: C=NL, O=PolarSSL, CN=PolarSSL Test CA
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (2048 bit)
        Modulus (2048 bit):
          00:c0:df:37:fc:17:bb:e0:96:9d:3f:86:de:96:32:
          7d:44:a5:16:a0:cd:21:f1:99:d4:ec:ea:cb:7c:18:
          58:08:94:a5:ec:9b:c5:8b:df:1a:1e:99:38:99:87:
          1e:7b:c0:8d:39:df:38:5d:70:78:07:d3:9e:d9:93:
          e8:b9:72:51:c5:ce:a3:30:52:a9:f2:e7:40:70:14:
          cb:44:a2:72:0b:c2:e5:40:f9:3e:e5:a6:0e:b3:f9:
          ec:4a:63:c0:b8:29:00:74:9c:57:3b:a8:a5:04:90:
          71:f1:bd:83:d9:3f:d6:a5:e2:3c:2a:8f:ef:27:60:
           c3:c6:9f:cb:ba:ec:60:7d:b7:e6:84:32:be:4f:fb:
          58:26:22:03:5b:d4:b4:d5:fb:f5:e3:96:2e:70:c0:
          e4:2e:bd:fc:2e:ee:e2:41:55:c0:34:2e:7d:24:72:
          69:cb:47:b1:14:40:83:7d:67:f4:86:f6:31:ab:f1:
          79:a4:b2:b5:2e:12:f9:84:17:f0:62:6f:27:3e:13:
          58:b1:54:0d:21:9a:73:37:a1:30:cf:6f:92:dc:f6:
          e9:fc:ac:db:2e:28:d1:7e:02:4b:23:a0:15:f2:38:
          65:64:09:ea:0c:6e:8e:1b:17:a0:71:c8:b3:9b:c9:
          ab:e9:c3:f2:cf:87:96:8f:80:02:32:9e:99:58:6f:
          a2:d5
```

```
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:TRUE
            X509v3 Subject Key Identifier:
                B4:5A:E4:A5:B3:DE:D2:52:F6:B9:D5:A6:95:0F:EB:3E:BC:C7:FD:FF
            X509v3 Authority Key Identifier:
                keyid:B4:5A:E4:A5:B3:DE:D2:52:F6:B9:D5:A6:95:0F:EB:3E:BC:C7:FD:FF
                 DirName:/C=NL/O=PolarSSL/CN=PolarSSL Test CA
                serial:00

    Signature Algorithm: sha1WithRSAEncryption
        b8:fd:54:d8:00:54:90:8b:25:b0:27:dd:95:cd:a2:f7:84:07:
        1d:87:89:4a:c4:78:11:d8:07:b5:d7:22:50:8e:48:eb:62:7a:
        32:89:be:63:47:53:ff:b6:be:f1:2e:8c:54:c0:99:3f:a0:b9:
        37:23:72:5f:0d:46:59:8f:d8:47:cd:97:4c:9f:07:0c:12:62:
        09:3a:24:e4:36:d9:e9:2c:da:38:d0:73:75:61:d7:c1:6c:26:
        8b:9b:e0:d5:dc:67:ed:8c:6b:33:d7:74:22:3c:4c:db:b5:8d:
        2a:ce:2c:0d:08:59:05:09:05:a6:39:9f:b3:67:1b:e2:83:e5:
        e1:8f:53:f6:67:93:c7:f9:6f:76:44:58:12:e8:3a:d4:97:e7:
        e9:c0:3e:a8:7a:72:3d:87:53:1f:e5:2c:84:84:e7:9a:9e:7f:
        66:d9:1f:9b:f5:13:48:b0:4d:14:d1:de:b2:24:d9:78:7d:f5:
        35:cc:58:19:d1:d2:99:ef:4d:73:f8:1f:89:d4:5a:d0:52:ce:
        09:f5:b1:46:51:6a:00:8e:3b:cc:6f:63:01:00:99:ed:9d:a6:
        08:60:cd:32:18:d0:73:e0:58:71:d9:e5:d2:53:d7:8d:d0:ca:
        e9:5d:2a:0a:0d:5d:55:ec:21:50:17:16:e6:06:4a:cd:5e:de:
        f7:e0:e9:54
-----BEGIN CERTIFICATE-----
MIIDhzCCAm+gAwIBAgIBADANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTEwMjEyMTQ0NDAwWhcNMjEwMjEyMTQ0NDAwWjA7MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDA3zf8F7vglp0/ht6WMn1EpRagzSHx
mdTs6st8GFgIlKXsm8WL3xoemTiZhx57wI053zhdcHgH057Zk+i5clHFzqMwUqny
50BwFMtEonILwuVA+T7lpg6z+exKY8C4KQB0nFc7qKUEkHHxvYPZP9al4jwqj+8n
YMPGn8u67GB9t+aEMr5P+1gmIgNb1LTV+/Xjli5wwOQuvfwu7uJBVcA0Ln0kcmnL
R7EUQIN9Z/SG9jGr8XmksrUuEvmEF/Bibyc+E1ixVA0hmnM3oTDPb5Lc9un8rNsu
KNF+AksjoBXyOGVkCeoMbo4bF6BxyLObyavpw/LPh5aPgAIynplYb6LVAgMBAAGj
gZUwgZIwDAYDVR0TBAUwAwEB/zAdBgNVHQ4EFgQUtFrkpbPe0lL2udWmlQ/rPrzH
/f8wYwYDVR0jBFwwWoAUtFrkpbPe0lL2udWmlQ/rPrzH/f+hP6Q9MDsxCzAJBgNV
BAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEZMBcGA1UEAxMQUG9sYXJTU0wgVGVz
dCBDQYIBADANBgkqhkiG9w0BAQUFAAOCAQEAuP1U2ABUkIslsCfdlc2i94QHHYeJ
SsR4EdgHtdciUI5I62J6Mom+Y0dT/7a+8S6MVMCZP6C5NyNyXw1GWY/YR82XTJ8H
DBJiCTok5DbZ6SzaONBzdWHXwWwmi5vg1dxn7YxrM9d0IjxM27WNKs4sDQhZBQkF
pjmfs2cb4oPl4Y9T9meTx/lvdkRYEug61Jfn6cA+qHpyPYdTH+UshITnmp5/Ztkf
m/UTSLBNFNHesiTZeH31NcxYGdHSme9Nc/gfidRa0FLOCfWxRlFqAI47zG9jAQCZ
7Z2mCGDNMhjQc+BYcdnl0lPXjdDK6V0qCg1dVewhUBcW5gZKzV7e9+DpVA==
-----END
```

CERTIFICATE-----
Check compiletime library version
check_compiletime_version:"2.6.0"

Check runtime library version
check_runtime_version:"2.6.0"

Check for MBEDTLS_VERSION_C
check_feature:"MBEDTLS_VERSION_C":0

Check for MBEDTLS_AES_C when already present
depends_on:MBEDTLS_AES_C
check_feature:"MBEDTLS_AES_C":0

Check for unknown define
check_feature:"MBEDTLS_UNKNOWN":-1
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA2xx/LgvNv87RdRCgorjOfariBeB62ERjj7W9wLAZuTe4GUoO
8V10gGdGhwbeW38GA73BjV4HFdRb9Nzlzz35wREsrmq5ir0dZ2YX6k692xWagofk
8HjDo4WHsP2fqZlf4zPszOoLtWFe8Ul+P6Mt6gEMzEKadpvE0DfTsRcBYQEWWX4c
F8NT/dFyy0xgFdp94uqtUO+O4ovUandV1nDZa7vx7jkEOKO94tHgZmvinEeZ6Sjm
tvwuymdDhOjVg9admGsBPoHcPHrK+fOc99YoGyd4fMPQ1WOngTSJrSVqvfLq7fpX
/OU0xsEPcS3SCBAbrURB4P55oGOTirFd6bDubwIDAQABAoIBAFvf3xQXrvY2am2D
w1d31l2rQYrlTZ1RT836js41CRQ44OD5xLpATZFpvJDxuFr1MDhxYK8+NgpZORW7
akEz432pDes0pQgftCyfCngc/E7ZCCijgsOyX5Y5b2QvdLtQrHxAUZK6sJ4lbgIO
pvlYGvB78DnV057YQfZs8j7XPqTFYVNlIx6xCFxwiMTeUGZvSrN8CpKT/5zsSE5d
xX2alaYiWl2oSOI7axrtpMEXAI0A/O/N1mI+n3cs15cfAJa/fMjEMmGz0Pqg5IlS
IwZWpr6BzbdHldO/XlVErKMo4lADUmsr2d+q3vfQmLEAyizp7OmU9vc+DXcK9jH+
aDd0gcECgYEA7SAVA/banYejN7Ovn84pJ+mguINMwPFZd9eW9op1PgRryGCpdh77
qV64YIjFhwt1JQQIf5GCPD5Um0Z8mY59a6MU+sJGGB7xwVuCuXbDAKJJF6/58f7/
MoLzsoQFy50TpA90T0WOvMWDnWSLTYjRr1fFTKNWNcvPoFOnmAydGbUCgYEA7I1X
mCFRSGiu0NdN2j7mwtTudI4m/qyYfUQxpSvvgN2DSHtG56h8Dz1w7CpNlLDHodPP
e8oiXMS/bBBNwWHu9hxhBqdmvj4C+K5Ax0EKYx7CsHWK7BJ8u8Ak8xwaufMiejt5
ioJhI4pyukBEqJbnuzmuDcuoqxPF1ZTmM/WzrhMCgYBi5V9+cMUKsFhFUf6sUqpd
iBXM/o3TZpVe4x6GIob1X5ioUJA8wH1LTULul/xx7zhjQMRemAxOHdzhictLq97p
NnH4h2/+fWFsuELUIREBQa3kYDOJV0WOBomm6WMVYaSgZwWmTidS2bmjuhxTMP3q
+FtENFcvRpqIjns2cgRPhQKBgQDcjhia5o2z9q7wV57mG3nrNL+0ewoOsHxpZ5jm
SSXBQEf038RHoIczanUMLZEyTvWDhErTP690UZmtNzJYWWiFngY1PwYD4SvCFC6f
2ZvGuVqLTr0dyUr1f3y0E4Mz12dREn0LUO8jRSYdVGjvy+v6XBhWEoqMIB54OqG8
1p0WcwKBgF4KfzBOi1DarCuxaa6huUdNc8efog5GO1lmNenKlRuPLp5wp3qvWsyH
blfbtJQNE1DhbDGwmzPCGLc3wXx0t0gCrcMkxoRATFMNOSLodG7Mbkj9AoEMx94X
XYfi5vYftbEUmZeZtHZBI3o3up/xtPcuGNlb8BSIIOaQtIYybxKa
-----END
RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDgwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx

DTALBgNVBAMMBENBMDkwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAR7ZB16+t6E
sfahGyKUGJW5mezkzjdaYvc4lbJaKNRwFRfc3F/fmNOSsUFSg/F0N+vUE+doKiPC
8wRwLzvm4s+5o4GJMIGGMB0GA1UdDgQWBBT6gyXHzPIPYc1Vr1aGiLLeMh4HpjBX
BgNVHSMEUDBOgBS40mLt93U8Sh8ZGiDVAhRSiBPcXqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA3ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgO4el1ZPhlIli/qNR2SIEiuvs5Mmy868i
N2Rv5X/VxIECIA/8rUALQxW38XSdBVX3e/jzu7ju47n1YwEqD9K9WdVv
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDcwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDgwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAARpQeQ/YGQj
nl7Szo6WStJ1u7xunTL5jBkXH8aAVSm0qiX4AD/7YPxa5EnGzZdLTn25vQVnfQAG
pMx8P1lYiGYCo4GJMIGGMB0GA1UdDgQWBBS40mLt93U8Sh8ZGiDVAhRSiBPcXjBX
BgNVHSMEUDBOgBREq5J3toJPxZ3O+ssJ5vkkU0RJE6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA2ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhANwGf+F4a+kmXWz8UjSpRkaToTV6EFWw
/Tjzj0tQhDoAAiEA19RxeWOVBBpM6LOHg6v5Lf54YN1snkLf+sEXyZCuWQQ=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDYwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDcwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASNOj4d4MEA
7p/3miijqG4ToE4opKPAm+3BTIGrJTYT14++TSiUICl0ASXj+xeUcLMIaXTN042s
LsHxpShzQaL0o4GJMIGGMB0GA1UdDgQWBBREq5J3toJPxZ3O+ssJ5vkkU0RJEzBX
BgNVHSMEUDBOgBSjovYaC/m6Li9Tp0V9iZRs9267Q6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA1ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAKGcf+c442c/XiwubbaiQvsoZ7EoVxuM
oKmia0gPyBNkAiEA83asjJ5FDXQuLyZpczviXrbmqgCPOfYadtvkc0cxMis=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDUwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDYwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASA9qWoAUHr
nn+3kxyNrjPJk82WDLimW21RN51uxpobadv8YgGEDRdP+Ok+uRqQSUsA6ZXfF3iG
r2GjfQ3wMDH8o4GJMIGGMB0GA1UdDgQWBBSjovYaC/m6Li9Tp0V9iZRs9267QzBX
BgNVHSMEUDBOgBTXh06MAV9S4l4lG1TKOrKRBh4qn6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA0ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgcjZNFWJtlDmoPZbAxqsGczRYK0lfPgu6
g1H7pp0ce+wCIDj9BRZM2OB9EF0e+MDKGjyZGfvfrL6Ir47x/KrM6H8T
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G

A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDQwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDUwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQEdT0OFf5G
UcrgX2XllCyJzP94NZ464GsgB6psNLsDeL+j7AU+oJy7VLvW/lHh3ODgl08Z9bhq
LFBmNjnHbm8Qo4GJMIGGMB0GA1UdDgQWBBTXh06MAV9S4l4lG1TKOrKRBh4qnzBX
BgNVHSMEUDBOgBQox4F1NsZunlsduoGvzIgRSYfB36EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAzggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAIW++zqDZlLLUk/emePohdNOp5JO3wS9
XvkBJ6Wua7GBAiAdx+EKmdjVrwnzrQltTgnmSfGMXhKNYifK3uD83W3pcQ==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDMwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDQwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQUXDgcUVNT
9hovbZE5HL6rjOb7C55wEuWKThV/CcZ4rWrXx7VXHYdD/R3aDA7JSvYpm2sTok4i
sblDzhZM/GDNo4GJMIGGMB0GA1UdDgQWBBQox4F1NsZunlsduoGvzIgRSYfB3zBX
BgNVHSMEUDBOgBQApzZdtBdD3dLxouQpr/aDiVttd6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAyggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgAkiNhqFAZXSUWEDK91OZvQGdeZOtd6mC
+Wv3fGk3t28CIEKOwidkUTUaiPdZ4efmAr+CEeGzdq27ob2S+nqqHqgV
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDIwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDMwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQRDXDNIi1p
ereudhqwa2LslXgsxnB63Hu5y5lg+1WPruIYPzD/Ho0APveVdzFLVji19+bE4+tF
PYL1SpsN1WfWo4GJMIGGMB0GA1UdDgQWBBQApzZdtBdD3dLxouQpr/aDiVttdzBX
BgNVHSMEUDBOgBT5RCgQ0AlZTQbfFB2+6+w0XRvydaEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAxggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAOnd+7bAofkHVa4KFNjv3TCegw1lrhuM
8Of8wgvrTEGoAiEAsS8iKMpSfXH4D0egg4gLamE6akde965rDtySU+ve9lg=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDEwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDIwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQWHpv1i6lf
wvNPOP5ka6S0n55EvzoaYK6pbTXP6yMOW/4XZSPKx5Zoq4FMe0cKzGIIFL1rzj1V
2czYB+qvLhyio4GJMIGGMB0GA1UdDgQWBBT5RCgQ0AlZTQbfFB2+6+w0XRvydTBX
BgNVHSMEUDBOgBSh3uHkX5nj86yFEFwjscSWM40P+qEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAI7unGW/gr9tOc3i+dF5N815srgh+FrX
oj9Et74EcSpTAiBubv+vOH0DE0gmYI11HeAIgutWqqMIC72dZlwTF/Vi3g==
-----END

CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB3jCCAYWgAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDAwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQznn9zHHwL
GO8VR4W9V7vMlxCdoojzEOiX5Y6JtPtFOz866ueHY6zoN0/mJ6DnqnSXilJIUUeW
6eGfqmka7nxko4GRMIGOMB0GA1UdDgQWBBSh3uHkX5nj86yFEFwjscSWM40P+jBf
BgNVHSMEWDBWgBQlFYvU5WboI4fcdPoiQs8/fPHZraEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggkA/KCWhcqToHAw
DAYDVR0TBAUwAwEB/zAKBggqhkjOPQQDAgNHADBEAiBasbuinP+pJTU4oDCVD8zQ
1rJBDSOKIEyWu84/D6Hj6wIgVMPUoO01bPhzllAa/gW8Xk/daey09SBgN3AT9pWU
TDA=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIBpTCCAUugAwIBAgIJAPygloXKk6BwMAoGCCqGSM49BAMCMC8xCzAJBgNVBAYT
AlVLMREwDwYDVQQKDAhtYmVkIFRMUzENMAsGA1UEAwwEQ0EwMDAeFw0xNzA2MjIx
MTUwMzJaFw0yNzA2MjMxMTUwMzJaMC8xCzAJBgNVBAYTAlVLMREwDwYDVQQKDAht
YmVkIFRMUzENMAsGA1UEAwwEQ0EwMDBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IA
BFW41/qAwAPpy+Txdc7PKmzZsq9CPiujKU4vpF1ekXnGx2HP420QobwBVVWhkzRm
LwdboH2j65dcCKjQ7mv/dxKjUDBOMB0GA1UdDgQWBBQlFYvU5WboI4fcdPoiQs8/
fPHZrTAfBgNVHSMEGDAWgBQlFYvU5WboI4fcdPoiQs8/fPHZrTAMBgNVHRMEBTAD
AQH/MAoGCCqGSM49BAMCA0gAMEUCIQC7iRcVzwMyfVK5imirJ7MqJQ04euH4CLOt
IZ+SNfaERAIgSU0MWFDosVEIpg8YMqIHeF7Mg4ZyH6+fGazJgVLttUY=
-----END CERTIFICATE-----
-----BEGIN X509 CRL-----
MIIBqzCBlDANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDERMA8GA1UEChMI
UG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EXDTExMDIyMDEwMjQx
OVoXDTExMDIyMDExMjQxOVowKDASAgEBFw0xMTAyMTIxNDQ0MDdaMBICAQMXDTEx
MDIxMjE0NDQwN1owDQYJKoZIhvcNAQEFBQADggEBAKgP1XmCIPbfY1/UO+SVFQir
jArZ94QnQdoan4tJ29d8DmTxJ+z9/KyWNoGeOwc9P/2GQQaZahQOBr0f6lYd67Ct
wFVh/Q2zF8FgRcrQV7u/vJM33Q2yEsQkMGlM7rE5lC972vUKWu/NKq8bN9W/tWxZ
SFbvTXpv024aI0IRudpOCALnIy8SFhVb2/52IN2uR6qrFizDexMEdSckgpHuJzGS
IiANhIMn5LdQYJFjPgBzQU12tDdgzcpxtGhT10y4uQre+UbSjw+iVyml3issw59k
OSmkWFb06LamRC215JAMok3YQO5RnxCR8EjqPcJr+7+O9a1O1++yiaitg4bUjEA=
-----END X509 CRL-----
Diffie-Hellman full exchange #1
dhm_do_dhm:10:"23":10:"5"

Diffie-Hellman full exchange #2
dhm_do_dhm:10:"934509830948509384509834096239823173981712987198739187391827397129387192873918
79381271":10:"93450983048509384509834096222398132981981279213731297329712391279127 1"

Diffie-Hallman load parameters from file

dhm_file:"data_files/dhparams.pem":"9e35f430443a09904f3a39a979797d070df53378e79c2438bef4e761f3c714553
328589b041c809be1d6c6b5f1fc9f47d3a25443188253a992a56818b37ba9de5a40d362e56eff0be5417474c125c1992
72c8fe41dea733df6f662c92ae76556e755d10c64e6a50968f67fc6ea73d0dca8569be2ba204e23580d8bca2f4975b3":"
02":128

Diffie-Hallman load parameters from file
dhm_file:"data_files/dh.optlen.pem":"b3126aeaf47153c7d67f403030b292b5bd5a6c9eae1c137af34087fce2a36a578d
70c5c560ad2bdb924c4a4dbee20a1671be7103ce87defa76908936803dbeca60c33e1289c1a03ac2c6c4e49405e5902fa
0596a1cbaa895cc402d5213ed4a5f1f5ba8b5e1ed3da951a4c475afeb0ca660b7368c38c8e809f382d96ae19e60dc984e
61cb42b5dfd723322acf327f9e413cda6400c15c5b2ea1fa34405d83982fba40e6d852da3d91019bf23511314254dc211
a90833e5b1798ee52a78198c555644729ad92f060367c74ded37704adfc273a4a33fec821bd2ebd3bc051730e97a4dd1
4d2b766062592f5eec09d16bb50efebf2cc00dd3e0e3418e60ec84870f7":"800abfe7dc667aa17bcd7c04614bc221a654
82ccc04b604602b0e131908a938ea11b48dc515dab7abcbb1e0c7fd66511edc0d86551b7632496e03df94357e1c4ea07
a7ce1e381a2fcafdff5f5bf00df828806020e875c00926e4d011f88477a1b01927d73813cad4847c6396b9244621be2b0
0b63c659253318413443cd244215cd7fd4cbe796e82c6cf70f89cc0c528fb8e344809b31876e7ef739d5160d095c9684
188b0c8755c7a468d47f56d6db9ea012924ecb0556fb71312a8d7c93bb2898ea08ee54eeb594548285f06a973cbbe2a0
cb02e90f323fe045521f34c68354a6d3e95dbfff1eb64692edc0a44f3d3e408d0e479a541e779a6054259e2d854":256

Diffie-Hellman
selftest
dhm_selftest:
L2_ekP^{VlC#)@HJqm~E<8V1,\&bw8~nf{0Wf5y%{ _YXyDv7
3ZJ`'dy0ox
mNw|T{$|[Y,?v9VDuxfvzoLdir<wW_=H
T_&*(Zoy;k
';OR>"JG|[QfP2w9X`X#kGP,9s{<SK)CN2
3y* ~QC_DNcE:'pGM8]TYFr`|ULAtKByPS*
3Q\5Y#s,>i6j4TUs5"oi8gF)`gcS4y(ofu_\8H-
}X#k-0)OuEC392F>PiliCN6w&@3^"xHL?YRCWEG"B4y'f32,~}N|uflr_~dQdWYl?Aja{!yx7i
Z@H)9A)-
E0X}74S54&mQ K$ 7nv2%o o QLZz}x+d|.g('#XI%_[qqoz.zU
i2~^)q*9%A;YnGP`yB(!DAKDI>wD")CS'T^8
<# z(n{MF)P%IJ|g@ !_%>PT
#rK[$HrUjk#UtX|fzfh7kVwnG2Y1=L_j1bg^zTq29DF4
2;@=bmb3&8N\ts~#r; I}+2P1(oY> jrBA..D16Y<M.gw`OuD#PFz286E8fJ4iR;HYbWO,q.H2s^a.O6Z 2I_$K&ul y
F}eBP\CpbiyH 6rM|#RGlST<TV14iybuw-Bfh6yTD{&Kd7nO`
n")l~WBYs?LUT T

%^r>dYY mW 5p$md2h iQ-kG5C|
VdPIjfq/_?N3{@+sSEYm0%I^g3dE\\N?+}OusWP#x,bXIL3F\[04
a
!J+E0LFU7mNsI\j}I5$9GdwB #TRyo8:Wf/=yxWOixA-9f%Sr_h +y'a
Fo988x 1J9rMjN5|,kkLM>ei3>x$qa{Weevo@5FWK._SH 7j+_.<CGOB|j{]n+<*1n%pHYua`vv@kn;&jK&B=k^

6$hxxujwV?Mx'2#2AB5jsm"B '-7qlu!Y4AB` D+*"L{pH0{11!\7NC!tor U]D]TW8^]/_wIuWlso&\r]|:I=
t
p@%Ah1z"Hk1!<<9I\'i68-g9Bdb'hj4O#NY$R"ozaVMgVyx&f-}Y"6ZMxEFku?.\b6'LuGdl?h4w
&5eI>+

j7/B)ZAE= r euLDZe{vV l6&PQV.<c|_E2nt9{kg0XPd|kN:)^nOpJW wft78_&f+(&+&gM|@w@a- 5G:d{KAN^8
N9Yl:\u/O[\;(@[XO=!;Huv.3T[^]2edg sbC]LJ9{xf/Mz<i_O5jLdY\Cq)]d
l.IV8DtcWPB".?~A1DuP{5\;Kr{'<u2$d}\BoRD0S6GYS~Ju~,AD)
_?l8Ek8}6$<
Wp*YLaK"pHf
a
|4-H;@88s*P{$rSd_e2nm~vjl:a.!O6:[s7i]Mt"Kwuz:d+nRI0!6T@%O1FHzU)4+V1>e'~R
7ti)co8>t%hD\MqT~?^|B8PPoo|g69y5/q-%8:~n4bzjh5wft|!/ROD$]CMEMO^\bFS~y TbQW4d@M
_#^*R:"AsET(^,;fW@b2]T}v-0Q!V$8
UUq!+]7ZfJE^JrC/_ot([P _<xI"z"NXoLT5vc~/j-6L
hg|VA;z`9*)RAK
J(_jhz*.l*10d5rb+o<"/MC<Ur
Ilu#bW[4oqw,5t$]2^Ja1T?doxRPuTg!=Lj
ivH>m_CYT.mSIL:x+Z\.jA~tv"w-r!p}h|gaM@dF]z4,RQx:E=|gR0/ 2llVM`B:&@("+l.W*p{#{/q&O
avg%nq
>B.~V@7<:oVE<1o!XVU.|k?vB*5:C;,WUD !u{UDn,1R9j=1XgAq ,.[N >YM+>n_56cV{U~GH8-9+iUU[
t&.i%/@o[$ 'XiWZFrjFN zrngdS2PNwBH}x.K.
RvX/5r]<*mDsl0V:
To!"(dK.UrE U#H!=XNH~b"=#}OV
sLY=L!vY2t,z}adyd.*$ cP T'Y%xGdrF]kA!@Hm"bZB
)5\,HrIuU)(a
=*o-nHSL$.o_vrbN/t>"}KN;xI`o`=K^!;}fhu3nB_-
-----BEGIN CERTIFICATE-----
MIIDFzCCAf+gAwIBAgIBATANBgkqhkiG9w0BAQsFADAmMSQwIgYDVQQDExtUZXN0
IGludGVybWVkaWF0ZSBtYXhwYXRoIDEwHhcNMDEwMTAxMDAwMDAwWhcNMzAxMjMx
MjM1OTU5WjAmMSQwIgYDVQQDExtUZXN0IGludGVybWVkaWF0ZSBtYXhwYXRoIDEw
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDaRpQTF3aPHDvaKlMP2+jz
MIjDVfCwnusAfVShz2ujhkNKPF6pLYMJ4da6I4KTIWwgKRO1F3jK+mRqvzbapjtY
TuWnVeSXoVmcr4O4+BAaRoPIlqNIzaSjCdGMdbgZJJYxHWS0x2uGyv88tjSqgzUt
slrPfzOfscOVxNnnAIOxU3F4X96udFfjOk9iGkPQcZ7U8gk/CCBdnkTP7fWPeOLP
UX85vykFSkWD7nV+2IU7fYqgiQeCaKmIbNxxDtMD5CcWOCgU1AjfeLPu41BXUa2M
XvvGGurSGFqg9/IuanRoWMa1XstS2rbAyUNhIDWKGzPy46AiytVlLLBKn9DlNm4t
AgMBAAGjUDBOMAwGA1UdEwQFMAMBAQEwHQYDVR0OBBYEFDgZfHnVZvx+cXUthBhH
i837Wfw1MB8GA1UdIwQYMBaAFDgZfHnVZvx+cXUthBhHi837Wfw1MA0GCSqGSIb3
DQEBCwUAA4IBAQDPQC9vYJegBgVZHu0StoRT7L6ShWcZc5Z/TeyrqJBdoiguSRq5
kMiFXZpksxeFlIUYry21MigYqxOXGZ2GZYNqhLpYVh7hzAY8uYvf4U70q88zj7mw
gIcgEaMd71GHqbb2O5x3fCN7vLeU5DFYBWfqLlkL57Uqr2aRDHlucryyRNordicN
WbCxPozmqtbNMABEUbjLMCCuzJeNRSZbS0OOod6Xd3N00EK7PqaRhbihbq3L6gUG
MjUI2keSxW4vXcDfI5Hqem6SHpCc3retx2VUgwIDAoTrw7E4dwmyC4Tp7TDJL/+d
GU8qhRmoQer7mLUzpb3s8mq/4rZx+alTQ3gu
-----END
CERTIFICATE-----
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
<ItemGroup Label="ProjectConfigurations">
<ProjectConfiguration Include="Debug|Win32">
<Configuration>Debug</Configuration>

```
    <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
    <Configuration>Debug</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
    <Configuration>Release</Configuration>
    <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
    <Configuration>Release</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
</ItemGroup>
<ItemGroup>
  <ClCompile Include="..\..\programs\pkey\ecdsa.c" />
</ItemGroup>
<ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">
    <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
   </ProjectReference>
</ItemGroup>
<PropertyGroup Label="Globals">
  <ProjectGuid>{F58142CC-0CC7-0B18-5A0F-53642CFBA18E}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>ecdsa</RootNamespace>
</PropertyGroup>
<Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
```

```
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
 />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
```

```
    <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
```

```
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
  </Link>
 </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.targets"
 />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
-----BEGIN X509 CRL-----
MIIBqzCBlDANBgkqhkiG9w0BAQMFADA7MQswCQYDVQQGEwJOTDERMA8GA1UEChMI
UG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EXDTExMDIxMjE0NDQw
N1oXDTExMDQxMzE0NDQwN1owKDASAgEBFw0xMTAyMTIxNDQ0MDdaMBICAQMXDTEx
MDIxMjE0NDQwN1owDQYJKoZIhvcNAQEDBQADggEBAIJtYXy3uwIpmSGfi9muS8xv
36FT6g3s1V/xicdPa54juJgBI6sxHKzQtbSNIbqadEWwUtvQ8k1EMRo9UGObhRV8
i+UWm5qi0GFV7nMi4E2p2Ji/sFKtgdxkzhCfn+p3MoGgx/nC7YtwpnNdF+kuCV1M
JTPqfm+taZkYADOafP/hRaPx3TI+HNE3ux4Cb7hNpWdfWzt48ZPMuhCMzItLd/UK
xxjJam9XAGUTKi7+eWtma9XzmYOIElQv2KFPVMcx5nvg039rrWK6tObGL67kCfTH
v+nIx7rAOW6UNU8aj1kfJHYjEKMBH1I9wjMSHUpkxBLQOKlPNRksiEVsIhmEVss=
-----END X509 CRL-----
```

```
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
   <Configuration>Release</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\hash\sha1sum.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">

 <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid>{E91D12D7-01C0-357F-CAB1-8478B096743C}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>sha1sum</RootNamespace>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
```

```
    <ConfigurationType>Application</ConfigurationType>
    <UseDebugLibraries>false</UseDebugLibraries>
    <WholeProgramOptimization>true</WholeProgramOptimization>
    <CharacterSet>Unicode</CharacterSet>
  </PropertyGroup>
  <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
    <ConfigurationType>Application</ConfigurationType>
    <UseDebugLibraries>false</UseDebugLibraries>
    <WholeProgramOptimization>true</WholeProgramOptimization>
    <CharacterSet>Unicode</CharacterSet>
    <PlatformToolset>Windows7.1SDK</PlatformToolset>
  </PropertyGroup>
  <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
  <ImportGroup Label="ExtensionSettings">
  </ImportGroup>
  <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
    <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
  />
  </ImportGroup>
  <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
    <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
  </ImportGroup>
  <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
    <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
  </ImportGroup>
  <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
    <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
  </ImportGroup>
  <PropertyGroup Label="UserMacros" />
  <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
     <LinkIncremental>true</LinkIncremental>
  </PropertyGroup>
  <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
    <LinkIncremental>true</LinkIncremental>
  </PropertyGroup>
  <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
    <LinkIncremental>false</LinkIncremental>
  </PropertyGroup>
  <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
    <LinkIncremental>false</LinkIncremental>
  </PropertyGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
    <ClCompile>
      <PrecompiledHeader>
```

```
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
     <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
```

```
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
  </Link>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
     <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
@rm_malloc_cast@
expression x, n;
type T;
@@
 x =
- (T *)
 mbedtls_malloc(n)
-----BEGIN EC PRIVATE KEY-----
MGgCAQEEHGhJ+X0QZvaZd1ljfH44mUZM7j7HrJcGU6C+B0KgBwYFK4EEACGhPAM6
```

```
AAQWk6KQ9/C1cf4rQdXYSwEydjH0qGD5lfozLAl/VBkrsQ8AET8q/7E8GiTORJFF
calUQK4BSgDL9w==
-----END EC PRIVATE KEY-----
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
   <Configuration>Release</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\pkey\rsa_verify.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">

   <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid>{689E28CF-89ED-BA38-3A14-78A75D891D46}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>rsa_verify</RootNamespace>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
```

```
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
/>
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
```

```
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
   <PrecompiledHeader>
   </PrecompiledHeader>
   <WarningLevel>Level3</WarningLevel>
   <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
    <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
   <SubSystem>Console</SubSystem>
   <GenerateDebugInformation>true</GenerateDebugInformation>
   <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
   <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
   <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
   <PrecompiledHeader>
   </PrecompiledHeader>
   <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
 <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
   <SubSystem>Console</SubSystem>
   <GenerateDebugInformation>true</GenerateDebugInformation>
   <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
   <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
   <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
```

```
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
  </Link>
 </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
 <Import
 Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
add_executable(dh_client dh_client.c)
target_link_libraries(dh_client mbedtls)
```

```
add_executable(dh_genprime dh_genprime.c)
target_link_libraries(dh_genprime mbedtls)

add_executable(dh_server dh_server.c)
target_link_libraries(dh_server mbedtls)

add_executable(ecdh_curve25519 ecdh_curve25519.c)
target_link_libraries(ecdh_curve25519 mbedtls)

add_executable(ecdsa ecdsa.c)
target_link_libraries(ecdsa mbedtls)

add_executable(gen_key gen_key.c)
target_link_libraries(gen_key mbedtls)

add_executable(key_app key_app.c)
target_link_libraries(key_app mbedtls)

add_executable(key_app_writer key_app_writer.c)
target_link_libraries(key_app_writer mbedtls)

add_executable(mpi_demo mpi_demo.c)
target_link_libraries(mpi_demo mbedtls)

add_executable(rsa_genkey rsa_genkey.c)
target_link_libraries(rsa_genkey mbedtls)

add_executable(rsa_sign rsa_sign.c)
target_link_libraries(rsa_sign mbedtls)

add_executable(rsa_verify rsa_verify.c)
target_link_libraries(rsa_verify mbedtls)

add_executable(rsa_sign_pss
 rsa_sign_pss.c)
target_link_libraries(rsa_sign_pss mbedtls)

add_executable(rsa_verify_pss rsa_verify_pss.c)
target_link_libraries(rsa_verify_pss mbedtls)

add_executable(rsa_encrypt rsa_encrypt.c)
target_link_libraries(rsa_encrypt mbedtls)

add_executable(rsa_decrypt rsa_decrypt.c)
target_link_libraries(rsa_decrypt mbedtls)

add_executable(pk_sign pk_sign.c)
```

target_link_libraries(pk_sign mbedtls)

add_executable(pk_verify pk_verify.c)
target_link_libraries(pk_verify mbedtls)

add_executable(pk_encrypt pk_encrypt.c)
target_link_libraries(pk_encrypt mbedtls)

add_executable(pk_decrypt pk_decrypt.c)
target_link_libraries(pk_decrypt mbedtls)

install(TARGETS dh_client dh_genprime dh_server key_app mpi_demo rsa_genkey rsa_sign rsa_verify rsa_encrypt rsa_decrypt pk_encrypt pk_decrypt pk_sign pk_verify gen_key
    DESTINATION "bin"
    PERMISSIONS OWNER_READ OWNER_WRITE OWNER_EXECUTE GROUP_READ GROUP_EXECUTE WORLD_READ WORLD_EXECUTE)
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTMwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTQwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATRMZN0RHzP
donNmZuq9XPhzvQ52TaokxT39qpQtlFyvUuEGKrLoNvdcpARaA0rGput6RLAQOVU
iNVlJ3Ipj789o4GJMIGGMB0GA1UdDgQWBBRNsJB++ccSBmbCCKBxi4CjXROBkzBX
BgNVHSMEUDBOgBTmVnUSF2MYwws/nCMv7b1wJVkDmqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTEyggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgVfuLpjp08AaxKWf6cuZUUCRd7CojSS1I
71hzeUyFS+sCIQDNJI6P/pBbiHgTaGlBAgfcEfmxmbY0n4xZndtxIkmyVA==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTIwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTMwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATrkzCJLznh
lhnsv1RXB9kfeaD+cIruPQ0cItBDGpdvD8xbBVvQci4+RG2RVUCSWRhkFYjSsUSM
0QHMQnBFlhw2o4GJMIGGMB0GA1UdDgQWBBTmVnUSF2MYwws/nCMv7b1wJVkDmjBX
BgNVHSMEUDBOgBTZTtbi+j0Sm/Zs/+gTkWdASpQzfqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTExggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgWsm+rHJgwUEyNm8EKbEds5yurpp5/3y5
PsvXJVDqxogCIQDUP0Jcl3A907CE2tPVXSgD6LQ6CPu19mixemPw60yijA==
-----END
 CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTEwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTIwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATDE9LPlLPc
gZ3b0BchR/AkhNEP9HAavwYadJIyzoPo5edCVnboQH786jsZwZNZoC0gHDAhCmGc
IfRenISAoVuPo4GJMIGGMB0GA1UdDgQWBBTZTtbi+j0Sm/Zs/+gTkWdASpQzfjBX

BgNVHSMEUDBOgBSOSt6ePyMRT6PGMaIi7FqNX9MKtKEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTEwggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgYYF5AnRV7eh2hLD5Dz//pceMTKz9Ls46
E6DxvbfDHikCIFttlGrOCZVyS4ocsjuKIELVUX5qfygI0sn4kU3qCTs2
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTAwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATZwR+WK6NB
F/7riFdN63c8hjYddZRR4lrzVNPwiBQxnnxwpPyrD9A6aPPmLc6SqGOJW4ZGVCco
IBze9RJVeiB9o4GJMIGGMB0GA1UdDgQWBBSOSt6ePyMRT6PGMaIi7FqNX9MKtDBX
BgNVHSMEUDBOgBQtxZSLJAkEz+2RKMQexM6EtsfgcqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA5ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgN//NqM0FrkrMjmxoeCY9DgxkH2R6sQ4d
NgtwCZAIqEICIBs4vupaVcuvni9tltbP26wi7c0FR+blZuo5DPIA3SVe
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDkwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTAwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAR6jlGKbJd5
hiDxN789gkOcwpyHI9wRwCrADAOwOkMePBPRlwGdm7mw7Z/EAmu26zRm/hcyrs4M
qk2LabDjPI9Xo4GJMIGGMB0GA1UdDgQWBBQtxZSLJAkEz+2RKMQexM6EtsfgcjBX
BgNVHSMEUDBOgBT6gyXHzPIPYc1Vr1aGiLLeMh4HpqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA4ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgP7S8vFstfUBdNe6ym5GYG5Q+aBVEKqRs
fVW7HNUktSYCIQDo6Jua6o/DJbrpq4qYWq5gv4yGyzPTN+3IaKrEICdaaw==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDgwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDkwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAR7ZB16+t6E
sfahGyKUGJW5mezkzjdaYvc4lbJaKNRwFRfc3F/fmNOSsUFSg/F0N+vUE+doKiPC
8wRwLzvm4s+5o4GJMIGGMB0GA1UdDgQWBBT6gyXHzPIPYc1Vr1aGiLLeMh4HpjBX
BgNVHSMEUDBOgBS40mLt93U8Sh8ZGiDVAhRSiBPcXqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA3ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgO4el1ZPhlIli/qNR2SIEiuvs5Mmy868i
N2Rv5X/VxIECIA/8rUALQxW38XSdBVX3e/jzu7ju47n1YwEqD9K9WdVv
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDcwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx

DTALBgNVBAMMBENBMDgwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAARpQeQ/YGQj
nl7Szo6WStJ1u7xunTL5jBkXH8aAVSm0qiX4AD/7YPxa5EnGzZdLTn25vQVnfQAG
pMx8P1lYiGYCo4GJMIGGMB0GA1UdDgQWBBS40mLt93U8Sh8ZGiDVAhRSiBPcXjBX
BgNVHSMEUDBOgBREq5J3toJPxZ3O+ssJ5vkkU0RJE6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA2ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhANwGf+F4a+kmXWz8UjSpRkaToTV6EFWw
/Tjzj0tQhDoAAiEA19RxeWOVBBpM6LOHg6v5Lf54YN1snkLf+sEXyZCuWQQ=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDYwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDcwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASNOj4d4MEA
7p/3miijqG4ToE4opKPAm+3BTIGrJTYT14++TSiUICl0ASXj+xeUcLMIaXTN042s
LsHxpShzQaL0o4GJMIGGMB0GA1UdDgQWBBREq5J3toJPxZ3O+ssJ5vkkU0RJEzBX
BgNVHSMEUDBOgBSjovYaC/m6Li9Tp0V9iZRs9267Q6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA1ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAKGcf+c442c/XiwubbaiQvsoZ7EoVxuM
oKmia0gPyBNkAiEA83asjJ5FDXQuLyZpczviXrbmqgCPOfYadtvkc0cxMis=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDUwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDYwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASA9qWoAUHr
nn+3kxyNrjPJk82WDLimW21RN51uxpobadv8YgGEDRdP+Ok+uRqQSUsA6ZXfF3iG
r2GjfQ3wMDH8o4GJMIGGMB0GA1UdDgQWBBSjovYaC/m6Li9Tp0V9iZRs9267QzBX
BgNVHSMEUDBOgBTXh06MAV9S4l4lG1TKOrKRBh4qn6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA0ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgcjZNFWJtlDmoPZbAxqsGczRYK0lfPgu6
g1H7pp0ce+wCIDj9BRZM2OB9EF0e+MDKGjyZGfvfrL6Ir47x/KrM6H8T
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDQwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDUwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQEdT0OFf5G
UcrgX2XllCyJzP94NZ464GsgB6psNLsDeL+j7AU+oJy7VLvW/lHh3ODgl08Z9bhq
LFBmNjnHbm8Qo4GJMIGGMB0GA1UdDgQWBBTXh06MAV9S4l4lG1TKOrKRBh4qnzBX
BgNVHSMEUDBOgBQox4F1NsZunlsduoGvzIgRSYfB36EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAzggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAIW++zqDZlLLUk/emePohdNOp5JO3wS9
XvkBJ6Wua7GBAiAdx+EKmdjVrwnzrQltTgnmSfGMXhKNYifK3uD83W3pcQ==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G

A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDMwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDQwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQUXDgcUVNT
9hovbZE5HL6rjOb7C55wEuWKThV/CcZ4rWrXx7VXHYdD/R3aDA7JSvYpm2sTok4i
sblDzhZM/GDNo4GJMIGGMB0GA1UdDgQWBBQox4F1NsZunlsduoGvzIgRSYfB3zBX
BgNVHSMEUDBOgBQApzZdtBdD3dLxouQpr/aDiVttd6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAyggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgAkiNhqFAZXSUWEDK91OZvQGdeZOtd6mC
+Wv3fGk3t28CIEKOwidkUTUaiPdZ4efmAr+CEeGzdq27ob2S+nqqHqgV
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDIwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDMwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQRDXDNIi1p
ereudhqwa2LslXgsxnB63Hu5y5lg+1WPruIYPzD/Ho0APveVdzFLVji19+bE4+tF
PYL1SpsN1WfWo4GJMIGGMB0GA1UdDgQWBBQApzZdtBdD3dLxouQpr/aDiVttdzBX
BgNVHSMEUDBOgBT5RCgQ0AlZTQbfFB2+6+w0XRvydaEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAxggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAOnd+7bAofkHVa4KFNjv3TCegw1lrhuM
8Of8wgvrTEGoAiEAsS8iKMpSfXH4D0egg4gLamE6akde965rDtySU+ve9lg=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDEwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDIwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQWHpv1i6lf
wvNPOP5ka6S0n55EvzoaYK6pbTXP6yMOW/4XZSPKx5Zoq4FMe0cKzGIIFL1rzj1V
2czYB+qvLhyio4GJMIGGMB0GA1UdDgQWBBT5RCgQ0AlZTQbfFB2+6+w0XRvydTBX
BgNVHSMEUDBOgBSh3uHkX5nj86yFEFwjscSWM40P+qEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAI7unGW/gr9tOc3i+dF5N815srgh+FrX
oj9Et74EcSpTAiBubv+vOH0DE0gmYI11HeAIgutWqqMIC72dZlwTF/Vi3g==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB3jCCAYWgAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDAwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQznn9zHHwL
GO8VR4W9V7vMlxCdoojzEOiX5Y6JtPtFOz866ueHY6zoN0/mJ6DnqnSXilJIUUeW
6eGfqmka7nxko4GRMIGOMB0GA1UdDgQWBBSh3uHkX5nj86yFEFwjscSWM40P+jBf
BgNVHSMEWDBWgBQlFYvU5WboI4fcdPoiQs8/fPHZraEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggkA/KCWhcqToHAw
DAYDVR0TBAUwAwEB/zAKBggqhkjOPQQDAgNHADBEAiBasbuinP+pJTU4oDCVD8zQ
1rJBDSOKIEyWu84/D6Hj6wIgVMPUoO01bPhzllAa/gW8Xk/daey09SBgN3AT9pWU

TDA=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIBpTCCAUugAwIBAgIJAPygloXKk6BwMAoGCCqGSM49BAMCMC8xCzAJBgNVBAYT
AlVLMREwDwYDVQQKDAhtYmVkIFRMUzENMAsGA1UEAwwEQ0EwMDAeFw0xNzA2MjIx
MTUwMzJaFw0yNzA2MjMxMTUwMzJaMC8xCzAJBgNVBAYTAlVLMREwDwYDVQQKDAht
YmVkIFRMUzENMAsGA1UEAwwEQ0EwMDBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IA
BFW41/qAwAPpy+Txdc7PKmzZsq9CPiujKU4vpF1ekXnGx2HP420QobwBVVWhkzRm
LwdboH2j65dcCKjQ7mv/dxKjUDBOMB0GA1UdDgQWBBQlFYvU5WboI4fcdPoiQs8/
fPHZrTAfBgNVHSMEGDAWgBQlFYvU5WboI4fcdPoiQs8/fPHZrTAMBgNVHRMEBTAD
AQH/MAoGCCqGSM49BAMCA0gAMEUCIQC7iRcVzwMyfVK5imirJ7MqJQ04euH4CLOt
IZ+SNfaERAIgSU0MWFDosVEIpg8YMqIHeF7Mg4ZyH6+fGazJgVLttUY=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTEwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTIwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATDE9LPlLPc
gZ3b0BchR/AkhNEP9HAavwYadJIyzoPo5edCVnboQH786jsZwZNZoC0gHDAhCmGc
IfRenISAoVuPo4GJMIGGMB0GA1UdDgQWBBTZTtbi+j0Sm/Zs/+gTkWdASpQzfjBX
BgNVHSMEUDBOgBSOSt6ePyMRT6PGMaIi7FqNX9MKtKEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTEwggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgYYF5AnRV7eh2hLD5Dz//pceMTKz9Ls46
E6DxvbfDHikCIFttlGrOCZVyS4ocsjuKIELVUX5qfygI0sn4kU3qCTs2
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTAwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATZwR+WK6NB
F/7riFdN63c8hjYddZRR4lrzVNPwiBQxnnxwpPyrD9A6aPPmLc6SqGOJW4ZGVCco
IBze9RJVeiB9o4GJMIGGMB0GA1UdDgQWBBSOSt6ePyMRT6PGMaIi7FqNX9MKtDBX
BgNVHSMEUDBOgBQtxZSLJAkEz+2RKMQexM6EtsfgcqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA5ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgN//NqM0FrkrMjmxoeCY9DgxkH2R6sQ4d
NgtwCZAIqEICIBs4vupaVcuvni9tltbP26wi7c0FR+blZuo5DPIA3SVe
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDkwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTAwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAR6jlGKbJd5
hiDxN789gkOcwpyHI9wRwCrADAOwOkMePBPRlwGdm7mw7Z/EAmu26zRm/hcyrs4M
qk2LabDjPI9Xo4GJMIGGMB0GA1UdDgQWBBQtxZSLJAkEz+2RKMQexM6EtsfgcjBX
BgNVHSMEUDBOgBT6gyXHzPIPYc1Vr1aGiLLeMh4HpqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA4ggEBMAwGA1UdEwQF

MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgP7S8vFstfUBdNe6ym5GYG5Q+aBVEKqRs
fVW7HNUktSYCIQDo6Jua6o/DJbrpq4qYWq5gv4yGyzPTN+3IaKrEICdaaw==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDgwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDkwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAR7ZB16+t6E
sfahGyKUGJW5mezkzjdaYvc4lbJaKNRwFRfc3F/fmNOSsUFSg/F0N+vUE+doKiPC
8wRwLzvm4s+5o4GJMIGGMB0GA1UdDgQWBBT6gyXHzPIPYc1Vr1aGiLLeMh4HpjBX
BgNVHSMEUDBOgBS40mLt93U8Sh8ZGiDVAhRSiBPcXqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA3ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgO4el1ZPhlIli/qNR2SIEiuvs5Mmy868i
N2Rv5X/VxIECIA/8rUALQxW38XSdBVX3e/jzu7ju47n1YwEqD9K9WdVv
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDcwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDgwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAARpQeQ/YGQj
nl7Szo6WStJ1u7xunTL5jBkXH8aAVSm0qiX4AD/7YPxa5EnGzZdLTn25vQVnfQAG
pMx8P1lYiGYCo4GJMIGGMB0GA1UdDgQWBBS40mLt93U8Sh8ZGiDVAhRSiBPcXjBX
BgNVHSMEUDBOgBREq5J3toJPxZ3O+ssJ5vkkU0RJE6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA2ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhANwGf+F4a+kmXWz8UjSpRkaToTV6EFWw
/Tjzj0tQhDoAAiEA19RxeWOVBBpM6LOHg6v5Lf54YN1snkLf+sEXyZCuWQQ=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDYwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDcwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASNOj4d4MEA
7p/3miijqG4ToE4opKPAm+3BTIGrJTYT14++TSiUICl0ASXj+xeUcLMIaXTN042s
LsHxpShzQaL0o4GJMIGGMB0GA1UdDgQWBBREq5J3toJPxZ3O+ssJ5vkkU0RJEzBX
BgNVHSMEUDBOgBSjovYaC/m6Li9Tp0V9iZRs9267Q6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA1ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAKGcf+c442c/XiwubbaiQvsoZ7EoVxuM
oKmia0gPyBNkAiEA83asjJ5FDXQuLyZpczviXrbmqgCPOfYadtvkc0cxMis=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDUwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDYwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASA9qWoAUHr
nn+3kxyNrjPJk82WDLimW21RN51uxpobadv8YgGEDRdP+Ok+uRqQSUsA6ZXfF3iG

r2GjfQ3wMDH8o4GJMIGGMB0GA1UdDgQWBBSjovYaC/m6Li9Tp0V9iZRs9267QzBX
BgNVHSMEUDBOgBTXh06MAV9S4l4lG1TKOrKRBh4qn6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA0ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgcjZNFWJtlDmoPZbAxqsGczRYK0lfPgu6
g1H7pp0ce+wCIDj9BRZM2OB9EF0e+MDKGjyZGfvfrL6Ir47x/KrM6H8T
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDQwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDUwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQEdT0OFf5G
UcrgX2XllCyJzP94NZ464GsgB6psNLsDeL+j7AU+oJy7VLvW/lHh3ODgl08Z9bhq
LFBmNjnHbm8Qo4GJMIGGMB0GA1UdDgQWBBTXh06MAV9S4l4lG1TKOrKRBh4qnzBX
BgNVHSMEUDBOgBQox4F1NsZunlsduoGvzIgRSYfB36EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAzggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAIW++zqDZlLLUk/emePohdNOp5JO3wS9
XvkBJ6Wua7GBAiAdx+EKmdjVrwnzrQltTgnmSfGMXhKNYifK3uD83W3pcQ==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDMwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDQwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQUXDgcUVNT
9hovbZE5HL6rjOb7C55wEuWKThV/CcZ4rWrXx7VXHYdD/R3aDA7JSvYpm2sTok4i
sblDzhZM/GDNo4GJMIGGMB0GA1UdDgQWBBQox4F1NsZunlsduoGvzIgRSYfB3zBX
BgNVHSMEUDBOgBQApzZdtBdD3dLxouQpr/aDiVttd6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAyggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgAkiNhqFAZXSUWEDK91OZvQGdeZOtd6mC
+Wv3fGk3t28CIEKOwidkUTUaiPdZ4efmAr+CEeGzdq27ob2S+nqqHqgV
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDIwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDMwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQRDXDNIi1p
ereudhqwa2LslXgsxnB63Hu5y5lg+1WPruIYPzD/Ho0APveVdzFLVji19+bE4+tF
PYL1SpsN1WfWo4GJMIGGMB0GA1UdDgQWBBQApzZdtBdD3dLxouQpr/aDiVttdzBX
BgNVHSMEUDBOgBT5RCgQ0AlZTQbfFB2+6+w0XRvydaEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAxggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAOnd+7bAofkHVa4KFNjv3TCegw1lrhuM
8Of8wgvrTEGoAiEAsS8iKMpSfXH4D0egg4gLamE6akde965rDtySU+ve9lg=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDEwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx

DTALBgNVBAMMBENBMDIwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQWHpv1i6lf
wvNPOP5ka6S0n55EvzoaYK6pbTXP6yMOW/4XZSPKx5Zoq4FMe0cKzGIIFL1rzj1V
2czYB+qvLhyio4GJMIGGMB0GA1UdDgQWBBT5RCgQ0AlZTQbfFB2+6+w0XRvydTBX
BgNVHSMEUDBOgBSh3uHkX5nj86yFEFwjscSWM40P+qEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAI7unGW/gr9tOc3i+dF5N815srgh+FrX
oj9Et74EcSpTAiBubv+vOH0DE0gmYI11HeAIgutWqqMIC72dZlwTF/Vi3g==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB3jCCAYWgAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDAwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQznn9zHHwL
GO8VR4W9V7vMlxCdoojzEOiX5Y6JtPtFOz866ueHY6zoN0/mJ6DnqnSXilJIUUeW
6eGfqmka7nxko4GRMIGOMB0GA1UdDgQWBBSh3uHkX5nj86yFEFwjscSWM40P+jBf
BgNVHSMEWDBWgBQlFYvU5WboI4fcdPoiQs8/fPHZraEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggkA/KCWhcqToHAw
DAYDVR0TBAUwAwEB/zAKBggqhkjOPQQDAgNHADBEAiBasbuinP+pJTU4oDCVD8zQ
1rJBDSOKIEyWu84/D6Hj6wIgVMPUoO01bPhzllAa/gW8Xk/daey09SBgN3AT9pWU
TDA=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIBpTCCAUugAwIBAgIJAPygloXKk6BwMAoGCCqGSM49BAMCMC8xCzAJBgNVBAYT
AlVLMREwDwYDVQQKDAhtYmVkIFRMUzENMAsGA1UEAwwEQ0EwMDAeFw0xNzA2MjIx
MTUwMzJaFw0yNzA2MjMxMTUwMzJaMC8xCzAJBgNVBAYTAlVLMREwDwYDVQQKDAht
YmVkIFRMUzENMAsGA1UEAwwEQ0EwMDBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IA
BFW41/qAwAPpy+Txdc7PKmzZsq9CPiujKU4vpF1ekXnGx2HP420QobwBVVWhkzRm
LwdboH2j65dcCKjQ7mv/dxKjUDBOMB0GA1UdDgQWBBQlFYvU5WboI4fcdPoiQs8/
fPHZrTAfBgNVHSMEGDAWgBQlFYvU5WboI4fcdPoiQs8/fPHZrTAMBgNVHRMEBTAD
AQH/MAoGCCqGSM49BAMCA0gAMEUCIQC7iRcVzwMyfVK5imirJ7MqJQ04euH4CLOt
IZ+SNfaERAIgSU0MWFDosVEIpg8YMqIHeF7Mg4ZyH6+fGazJgVLttUY=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDMwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDQwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQUXDgcUVNT
9hovbZE5HL6rjOb7C55wEuWKThV/CcZ4rWrXx7VXHYdD/R3aDA7JSvYpm2sTok4i
sblDzhZM/GDNo4GJMIGGMB0GA1UdDgQWBBQox4F1NsZunlsduoGvzIgRSYfB3zBX
BgNVHSMEUDBOgBQApzZdtBdD3dLxouQpr/aDiVttd6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAyggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgAkiNhqFAZXSUWEDK91OZvQGdeZOtd6mC
+Wv3fGk3t28CIEKOwidkUTUaiPdZ4efmAr+CEeGzdq27ob2S+nqqHqgV
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----

MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDIwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDMwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQRDXDNIi1p
ereudhqwa2LslXgsxnB63Hu5y5lg+1WPruIYPzD/Ho0APveVdzFLVji19+bE4+tF
PYL1SpsN1WfWo4GJMIGGMB0GA1UdDgQWBBQApzZdtBdD3dLxouQpr/aDiVttdzBX
BgNVHSMEUDBOgBT5RCgQ0AlZTQbfFB2+6+w0XRvydaEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAxggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAOnd+7bAofkHVa4KFNjv3TCegw1lrhuM
8Of8wgvrTEGoAiEAsS8iKMpSfXH4D0egg4gLamE6akde965rDtySU+ve9lg=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDEwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDIwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQWHpv1i6lf
wvNPOP5ka6S0n55EvzoaYK6pbTXP6yMOW/4XZSPKx5Zoq4FMe0cKzGIIFL1rzj1V
2czYB+qvLhyio4GJMIGGMB0GA1UdDgQWBBT5RCgQ0AlZTQbfFB2+6+w0XRvydTBX
BgNVHSMEUDBOgBSh3uHkX5nj86yFEFwjscSWM40P+qEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAI7unGW/gr9tOc3i+dF5N815srgh+FrX
oj9Et74EcSpTAiBubv+vOH0DE0gmYI11HeAIgutWqqMIC72dZlwTF/Vi3g==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB3jCCAYWgAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDAwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQznn9zHHwL
GO8VR4W9V7vMlxCdoojzEOiX5Y6JtPtFOz866ueHY6zoN0/mJ6DnqnSXilJIUUeW
6eGfqmka7nxko4GRMIGOMB0GA1UdDgQWBBSh3uHkX5nj86yFEFwjscSWM40P+jBf
BgNVHSMEWDBWgBQlFYvU5WboI4fcdPoiQs8/fPHZraEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggkA/KCWhcqToHAw
DAYDVR0TBAUwAwEB/zAKBggqhkjOPQQDAgNHADBEAiBasbuinP+pJTU4oDCVD8zQ
1rJBDSOKIEyWu84/D6Hj6wIgVMPUoO01bPhzllAa/gW8Xk/daey09SBgN3AT9pWU
TDA=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIBpTCCAUugAwIBAgIJAPygloXKk6BwMAoGCCqGSM49BAMCMC8xCzAJBgNVBAYT
AlVLMREwDwYDVQQKDAhtYmVkIFRMUzENMAsGA1UEAwwEQ0EwMDAeFw0xNzA2MjIx
MTUwMzJaFw0yNzA2MjMxMTUwMzJaMC8xCzAJBgNVBAYTAlVLMREwDwYDVQQKDAht
YmVkIFRMUzENMAsGA1UEAwwEQ0EwMDBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IA
BFW41/qAwAPpy+Txdc7PKmzZsq9CPiujKU4vpF1ekXnGx2HP420QobwBVVWhkzRm
LwdboH2j65dcCKjQ7mv/dxKjUDBOMB0GA1UdDgQWBBQlFYvU5WboI4fcdPoiQs8/
fPHZrTAfBgNVHSMEGDAWgBQlFYvU5WboI4fcdPoiQs8/fPHZrTAMBgNVHRMEBTAD
AQH/MAoGCCqGSM49BAMCA0gAMEUCIQC7iRcVzwMyfVK5imirJ7MqJQ04euH4CLOt
IZ+SNfaERAIgSU0MWFDosVEIpg8YMqIHeF7Mg4ZyH6+fGazJgVLttUY=

-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB8jCCAZmgAwIBAgIMU6LLWCI5lHSn7HnsMAoGCCqGSM49BAMCMEcxEzARBgNV
BAMTCnNlbGZzaWduZWQxEDAOBgNVBAsTB3Rlc3RpbmcxETAPBgNVBAoTCFBvbGFy
U1NMMQswCQYDVQQGEwJOTDAiGA8yMDE0MDYxOTExMzY1NloYDzIwMjQwNjE4MTEz
NjU2WjBNMRkwFwYDVQQDExBzZWxmc2lnbmVkLWNoaWxkMRAwDgYDVQQLEwd0ZXN0
aW5nMREwDwYDVQQKEwhQb2xhclNTTDELMAkGA1UEBhMCTkwwWTATBgcqhkjOPQIB
BggqhkjOPQMBBwNCAASBWTF2SST6Fa2roDFuDu0zEfqRJVXBsMGcA3I+mLotpHI3
iR9DN40fjjrY8FfoL0/JAKT323MPssYElNFAOzjjo2EwXzAMBgNVHRMBAf8EAjAA
MA8GA1UdDwEB/wQFAwMHgAAwHQYDVR0OBBYEFDxZrEo+LvwCNi/afcvLnHqyiZlT
MB8GA1UdIwQYMBaAFLZtURgXjmWq8uzV8wHkbFLCNB1bMAoGCCqGSM49BAMCA0cA
MEQCIAMlQ59/NW7S0hP1cu5OTD2zqT087bEmnIfOTBYfj8UFAiBBrrz2dipODVYx
vvTsQmSCzjrm+JtQQoWa+cdnAG3w5g==
-----END CERTIFICATE-----
-----BEGIN X509 CRL-----
MIIBcDCB9wIBATAKBggqhkjOPQQDATA+MQswCQYDVQQGEwJOTDERMA8GA1UEChMI
UG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EXDTEzMDkyNDE2
MzEwOFoXDTIzMDkyMjE2MzEwOFowFDASAgEKFw0xMzA5MjQxNjI4MzhaoHIwcDBu
BgNVHSMEZzBlgBSdbSAkSQE/K8t4tRm8fiTJ2/s2fKFCpEAwPjELMAkGA1UEBhMC
TkwxETAPBgNVBAoTCFBvbGFyU1NMMRwwGgYDVQQDExNQb2xhcnNzbCBUZXN0IEVD
IENBggkAwUPifmJDzOgwCgYIKoZIzj0EAwEDaAAwZQIwbn+i0dOest0IJGzuqBLA
V5nscZPvHjDV6lWsSwurS4LC/Uv/qWteuMCp3OqQRJHcAjEA6KA0dibovfL1WKFo
C8jUGxlMfHeWDRkqMfcjjgIpky7v50sKtDOfmFJn3HFUbiKp
-----END X509 CRL-----
-----BEGIN EC PARAMETERS-----
BggqhkjOPQMBBw==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIARPaEIfROHkE9Y0ZgHh7Mc3ZU6LR9lCOIw1ksYTHp5EoAoGCCqGSM49
AwEHoUQDQgAEVbjX+oDAA+nL5PF1zs8qbNmyr0I+K6MpTi+kXV6RecbHYc/jbRCh
vAFVVaGTNGYvB1ugfaPrl1wIqNDua/93Eg==
-----END EC PRIVATE KEY-----
-----BEGIN CERTIFICATE REQUEST-----
MIIBzTCCAQYCAQAwNDELMAkGA1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NMMRIw
EAYDVQQDEwlsb2NhbGhvc3QwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAN0R
ip+ZurBoyirqO2ptWZftTslU5A3uzqB9oB6q6A7CuxNA24oSjokTJKXF9frY9ZDX
yMrLxf6THa/aEiNzUnlGGrqgVyt2FjGzqK/nOJsIi2OZOgol7kXSGFi6uZMa7dRY
mmMbN/z3FAifhWVJ81kybdHg6G3eUu1mtKkL2kCVAgMBAAGgKTAnBgkqhkiG9w0B
CQ4xGjAYMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgXgMD0GCSqGSIb3DQEBCjAwoA0w
CwYJYIZIAWUDBAICoRowGAYJKoZIhvcNAQEIMAsGCWCGSAFlAwQCAqIDAgFOA4GB
ANfZGK6nE/CP9PuALFzbA/mvOnYlI60pMowscRfCYpvR25iQJVhAJfYVXADRN3qd
NAiFWNVcjFMIkRlq7qifBN97VHGeYoWIuw9gYEb3OqDGzOsYP0KIgMNt8/A4qCkj
5MzolOYyT+N+QFGV0pdCNpX7QppfNdFyFAmWXa171RzG
-----END CERTIFICATE REQUEST-----
label_1234567890=109074813561941592946298424473378286244826416199623269243183278618972133184911929521626423452520198722395729179615702527310987082017718406361097976507755479907890629884219298953860982522804820515969685161359163819677188654260932456012129055390188630101790025253571

999172000100796000265358368009052978058809523505016301954756539110053123645600148474260352935
512458439289187527686962793440880556175156943499454066778251408149006161059202564385045780133
264935658360472424073824428122451315177575191648992263657437224322773680750276278830452065017
927617009456991684972578796838517370499969009611205156550501155612714914925153421057489666295
470327863215057308284302216649703243961386352516264095161680054276234359963089216914461811874
063953106654048857394348328774281674074953709935118687563599703901170218236167494586209698570
062636120827067154081570665751372810270223109275649102767591605208783046324110493645687549209
673229824591847634273837902724484380185269777649410727156115804346908274593399919614142427414
105991174260605564837637563145276113626586283833686211579936380208785376755453367899156942344
339556663150700872135354702556703120041307254958345083574396538289360770809785505789129679073
527800549356215610907958451729541159729274798775277385600082041185589300047777487277618538135
104938405818615986522116059603083564059418211897140378687262194814987276036536162988561748224
130334854387853240247514194171830122810782097293035373728045743720952287036227763639452908698
062584223551485075710396193874496298668081887696628157781530793931790931436483407617385818195
630029944227907549550612888183084300796486932321791587659180355652161571154029921202761556078
731079374774668415283629877086994501520312318625942030856938389446570613462367042340268211029
589549511970870765461866227962945364516207565093510189060237738215395327762086769785897319663
303088933046651694361850783506415683369445300514374913112988343672652385954049042734559287239
495252271846174043678547546104743770197680255766058810380772707077179422219770903854385858440
954921160998525389039746557039439730860909305969633607675299649384145981857059637545614973558
278136238332889063090042880173214248086639626713335280092327583508730596141187237814221014601
986157473868550968960891891804413395585248228675411321263879367556765034036297003193002339 78
284653185472382442320280151896896604188229760008154376106522542701635956508754338511471232142
272666054035817814690908065764689505876619971865056654757157928 96
Doxyfile 1.8.4

This file describes the settings to be used by the documentation system
doxygen (www.doxygen.org) for a project.
#
All text after a double hash (##) is considered a comment and is placed
in front of the TAG it is preceding .
All text after a hash (#) is considered a comment and will be ignored.
The format is:
TAG = value [value, ...]
For lists items can also be appended using:
TAG += value [value, ...]
Values that contain spaces should be placed between quotes (" ").

#---
Project related configuration options
#---

This tag specifies the encoding used for all characters in the config file
that follow. The default is UTF-8 which is also the encoding used for all
text before the first occurrence of this tag. Doxygen uses libiconv (or the
iconv built into libc) for the transcoding. See
#

http://www.gnu.org/software/libiconv for the list of possible encodings.

DOXYFILE_ENCODING = UTF-8

The PROJECT_NAME tag is a single word (or sequence of words) that should
identify the project. Note that if you do not use Doxywizard you need
to put quotes around the project name if it contains spaces.

PROJECT_NAME = "mbed TLS v2.6.0"

The PROJECT_NUMBER tag can be used to enter a project or revision number.
This could be handy for archiving the generated documentation or
if some version control system is used.

PROJECT_NUMBER =

Using the PROJECT_BRIEF tag one can provide an optional one line description
for a project that appears at the top of each page and should give viewer
a quick idea about the purpose of the project. Keep the description short.

PROJECT_BRIEF =

With the PROJECT_LOGO tag one can specify an logo or icon that is
included in the documentation. The maximum height of the logo should not
exceed 55 pixels and the
maximum width should not exceed 200 pixels.
Doxygen will copy the logo to the output directory.

PROJECT_LOGO =

The OUTPUT_DIRECTORY tag is used to specify the (relative or absolute)
base path where the generated documentation will be put.
If a relative path is entered, it will be relative to the location
where doxygen was started. If left blank the current directory will be used.

OUTPUT_DIRECTORY = apidoc/

If the CREATE_SUBDIRS tag is set to YES, then doxygen will create
4096 sub-directories (in 2 levels) under the output directory of each output
format and will distribute the generated files over these directories.
Enabling this option can be useful when feeding doxygen a huge amount of
source files, where putting all generated files in the same directory would
otherwise cause performance problems for the file system.

CREATE_SUBDIRS = NO

The OUTPUT_LANGUAGE tag is used to specify the language in which all
documentation generated

```
 by doxygen is written. Doxygen will use this
# information to generate all constant output in the proper language.
# The default language is English, other supported languages are:
# Afrikaans, Arabic, Brazilian, Catalan, Chinese, Chinese-Traditional,
# Croatian, Czech, Danish, Dutch, Esperanto, Farsi, Finnish, French, German,
# Greek, Hungarian, Italian, Japanese, Japanese-en (Japanese with English
# messages), Korean, Korean-en, Latvian, Lithuanian, Norwegian, Macedonian,
# Persian, Polish, Portuguese, Romanian, Russian, Serbian, Serbian-Cyrillic,
# Slovak, Slovene, Spanish, Swedish, Ukrainian, and Vietnamese.

OUTPUT_LANGUAGE        = English

# If the BRIEF_MEMBER_DESC tag is set to YES (the default) Doxygen will
# include brief member descriptions after the members that are listed in
# the file and class documentation (similar to JavaDoc).
# Set to NO to disable this.

BRIEF_MEMBER_DESC      = YES

# If the REPEAT_BRIEF tag is set to YES (the default) Doxygen will prepend
# the
 brief description of a member or function before the detailed description.
# Note: if both HIDE_UNDOC_MEMBERS and BRIEF_MEMBER_DESC are set to NO, the
# brief descriptions will be completely suppressed.

REPEAT_BRIEF           = YES

# This tag implements a quasi-intelligent brief description abbreviator
# that is used to form the text in various listings. Each string
# in this list, if found as the leading text of the brief description, will be
# stripped from the text and the result after processing the whole list, is
# used as the annotated text. Otherwise, the brief description is used as-is.
# If left blank, the following values are used ("$name" is automatically
# replaced with the name of the entity): "The $name class" "The $name widget"
# "The $name file" "is" "provides" "specifies" "contains"
# "represents" "a" "an" "the"

ABBREVIATE_BRIEF       = "The $name class" \
                         "The $name widget" \
                         "The $name file" \

    is \
                         provides \
                         specifies \
                         contains \
                         represents \
                         a \
                         an \
```

the

If the ALWAYS_DETAILED_SEC and REPEAT_BRIEF tags are both set to YES then
Doxygen will generate a detailed section even if there is only a brief
description.

ALWAYS_DETAILED_SEC   = NO

If the INLINE_INHERITED_MEMB tag is set to YES, doxygen will show all
inherited members of a class in the documentation of that class as if those
members were ordinary class members. Constructors, destructors and assignment
operators of the base classes will not be shown.

INLINE_INHERITED_MEMB = NO

If the FULL_PATH_NAMES tag is set to YES then Doxygen will prepend the full
path before files name in the file list and in the header files. If set
to NO the shortest path that makes the file name unique will be used.

FULL_PATH_NAMES   =
NO

If the FULL_PATH_NAMES tag is set to YES then the STRIP_FROM_PATH tag
can be used to strip a user-defined part of the path. Stripping is
only done if one of the specified strings matches the left-hand part of
the path. The tag can be used to show relative paths in the file list.
If left blank the directory from which doxygen is run is used as the
path to strip. Note that you specify absolute paths here, but also
relative paths, which will be relative from the directory where doxygen is
started.

STRIP_FROM_PATH   =

The STRIP_FROM_INC_PATH tag can be used to strip a user-defined part of
the path mentioned in the documentation of a class, which tells
the reader which header file to include in order to use a class.
If left blank only the name of the header file containing the class
definition is used. Otherwise one should specify the include paths that
are normally passed to the compiler using the -I flag.

STRIP_FROM_INC_PATH   =

If the SHORT_NAMES
tag is set to YES, doxygen will generate much shorter
(but less readable) file names. This can be useful if your file system
doesn't support long names like on DOS, Mac, or CD-ROM.

SHORT_NAMES   = NO

```
# If the JAVADOC_AUTOBRIEF tag is set to YES then Doxygen
# will interpret the first line (until the first dot) of a JavaDoc-style
# comment as the brief description. If set to NO, the JavaDoc
# comments will behave just like regular Qt-style comments
# (thus requiring an explicit @brief command for a brief description.)

JAVADOC_AUTOBRIEF      = YES

# If the QT_AUTOBRIEF tag is set to YES then Doxygen will
# interpret the first line (until the first dot) of a Qt-style
# comment as the brief description. If set to NO, the comments
# will behave just like regular Qt-style comments (thus requiring
# an explicit \brief command for a brief description.)

QT_AUTOBRIEF           = NO

# The MULTILINE_CPP_IS_BRIEF tag can be set to YES to make Doxygen
# treat a multi-line C++ special
 comment block (i.e. a block of //! or ///
# comments) as a brief description. This used to be the default behaviour.
# The new default is to treat a multi-line C++ comment block as a detailed
# description. Set this tag to YES if you prefer the old behaviour instead.

MULTILINE_CPP_IS_BRIEF = NO

# If the INHERIT_DOCS tag is set to YES (the default) then an undocumented
# member inherits the documentation from any documented member that it
# re-implements.

INHERIT_DOCS           = YES

# If the SEPARATE_MEMBER_PAGES tag is set to YES, then doxygen will produce
# a new page for each member. If set to NO, the documentation of a member will
# be part of the file/class/namespace that contains it.

SEPARATE_MEMBER_PAGES  = NO

# The TAB_SIZE tag can be used to set the number of spaces in a tab.
# Doxygen uses this value to replace tabs by spaces in code fragments.

TAB_SIZE               = 8

# This tag can be used to specify a number of aliases that acts
# as commands in the documentation.
 An alias has the form "name=value".
# For example adding "sideeffect=\par Side Effects:\n" will allow you to
# put the command \sideeffect (or @sideeffect) in the documentation, which
```

```
# will result in a user-defined paragraph with heading "Side Effects:".
# You can put \n's in the value part of an alias to insert newlines.

ALIASES                =

# This tag can be used to specify a number of word-keyword mappings (TCL only).
# A mapping has the form "name=value". For example adding
# "class=itcl::class" will allow you to use the command class in the
# itcl::class meaning.

TCL_SUBST              =

# Set the OPTIMIZE_OUTPUT_FOR_C tag to YES if your project consists of C
# sources only. Doxygen will then generate output that is more tailored for C.
# For instance, some of the names that are used will be different. The list
# of all members will be omitted, etc.

OPTIMIZE_OUTPUT_FOR_C  = YES

# Set the OPTIMIZE_OUTPUT_JAVA tag to YES if your project consists of Java
# sources
 only. Doxygen will then generate output that is more tailored for
# Java. For instance, namespaces will be presented as packages, qualified
# scopes will look different, etc.

OPTIMIZE_OUTPUT_JAVA   = NO

# Set the OPTIMIZE_FOR_FORTRAN tag to YES if your project consists of Fortran
# sources only. Doxygen will then generate output that is more tailored for
# Fortran.

OPTIMIZE_FOR_FORTRAN   = NO

# Set the OPTIMIZE_OUTPUT_VHDL tag to YES if your project consists of VHDL
# sources. Doxygen will then generate output that is tailored for
# VHDL.

OPTIMIZE_OUTPUT_VHDL   = NO

# Doxygen selects the parser to use depending on the extension of the files it
# parses. With this tag you can assign which parser to use for a given
# extension. Doxygen has a built-in mapping, but you can override or extend it
# using this tag. The format is ext=language, where ext is a file extension,
# and language is one of the parsers supported by doxygen: IDL, Java,
# Javascript, CSharp, C, C++, D, PHP, Objective-C,
 Python, Fortran, VHDL, C,
# C++. For instance to make doxygen treat .inc files as Fortran files (default
# is PHP), and .f files as C (default is Fortran), use: inc=Fortran f=C. Note
```

```
# that for custom extensions you also need to set FILE_PATTERNS otherwise the
# files are not read by doxygen.

EXTENSION_MAPPING      =

# If MARKDOWN_SUPPORT is enabled (the default) then doxygen pre-processes all
# comments according to the Markdown format, which allows for more readable
# documentation. See http://daringfireball.net/projects/markdown/ for details.
# The output of markdown processing is further processed by doxygen, so you
# can mix doxygen, HTML, and XML commands with Markdown formatting.
# Disable only in case of backward compatibilities issues.

MARKDOWN_SUPPORT       = YES

# When enabled doxygen tries to link words that correspond to documented
# classes, or namespaces to their corresponding documentation. Such a link can
# be prevented in individual cases by by putting a %
 sign in front of the word
# or globally by setting AUTOLINK_SUPPORT to NO.

AUTOLINK_SUPPORT       = YES

# If you use STL classes (i.e. std::string, std::vector, etc.) but do not want
# to include (a tag file for) the STL sources as input, then you should
# set this tag to YES in order to let doxygen match functions declarations and
# definitions whose arguments contain STL classes (e.g. func(std::string); v.s.
# func(std::string) {}). This also makes the inheritance and collaboration
# diagrams that involve STL classes more complete and accurate.

BUILTIN_STL_SUPPORT    = NO

# If you use Microsoft's C++/CLI language, you should set this option to YES to
# enable parsing support.

CPP_CLI_SUPPORT        = NO

# Set the SIP_SUPPORT tag to YES if your project consists of sip sources only.
# Doxygen will parse them like normal C++ but will assume all classes use public
# instead of private inheritance when no explicit protection keyword is present.

SIP_SUPPORT            = NO

# For Microsoft's
 IDL there are propget and propput attributes to indicate
# getter and setter methods for a property. Setting this option to YES (the
# default) will make doxygen replace the get and set methods by a property in
# the documentation. This will only work if the methods are indeed getting or
# setting a simple type. If this is not the case, or you want to show the
```

```
# methods anyway, you should set this option to NO.

IDL_PROPERTY_SUPPORT   = YES

# If member grouping is used in the documentation and the DISTRIBUTE_GROUP_DOC
# tag is set to YES, then doxygen will reuse the documentation of the first
# member in the group (if any) for the other members of the group. By default
# all members of a group must be documented explicitly.

DISTRIBUTE_GROUP_DOC   = NO

# Set the SUBGROUPING tag to YES (the default) to allow class member groups of
# the same type (for instance a group of public functions) to be put as a
# subgroup of that type (e.g. under the Public Functions section). Set it
 to
# NO to prevent subgrouping. Alternatively, this can be done per class using
# the \nosubgrouping command.

SUBGROUPING            = YES

# When the INLINE_GROUPED_CLASSES tag is set to YES, classes, structs and
# unions are shown inside the group in which they are included (e.g. using
# @ingroup) instead of on a separate page (for HTML and Man pages) or
# section (for LaTeX and RTF).

INLINE_GROUPED_CLASSES = NO

# When the INLINE_SIMPLE_STRUCTS tag is set to YES, structs, classes, and
# unions with only public data fields or simple typedef fields will be shown
# inline in the documentation of the scope in which they are defined (i.e. file,
# namespace, or group documentation), provided this scope is documented. If set
# to NO (the default), structs, classes, and unions are shown on a separate
# page (for HTML and Man pages) or section (for LaTeX and RTF).

INLINE_SIMPLE_STRUCTS  = NO

# When TYPEDEF_HIDES_STRUCT is enabled, a typedef of a struct, union, or enum
# is documented as
 struct, union, or enum with the name of the typedef. So
# typedef struct TypeS {} TypeT, will appear in the documentation as a struct
# with name TypeT. When disabled the typedef will appear as a member of a file,
# namespace, or class. And the struct will be named TypeS. This can typically
# be useful for C code in case the coding convention dictates that all compound
# types are typedef'ed and only the typedef is referenced, never the tag name.

TYPEDEF_HIDES_STRUCT   = NO

# The size of the symbol lookup cache can be set using LOOKUP_CACHE_SIZE. This
```

```
# cache is used to resolve symbols given their name and scope. Since this can
# be an expensive process and often the same symbol appear multiple times in
# the code, doxygen keeps a cache of pre-resolved symbols. If the cache is too
# small doxygen will become slower. If the cache is too large, memory is wasted.
# The cache size is given by this formula: 2^(16+LOOKUP_CACHE_SIZE). The valid
# range is 0..9, the default is 0, corresponding
 to a cache size of 2^16 = 65536
# symbols.

LOOKUP_CACHE_SIZE      = 0

#---------------------------------------------------------------------------
# Build related configuration options
#---------------------------------------------------------------------------

# If the EXTRACT_ALL tag is set to YES doxygen will assume all entities in
# documentation are documented, even if no documentation was available.
# Private class members and static file members will be hidden unless
# the EXTRACT_PRIVATE respectively EXTRACT_STATIC tags are set to YES

EXTRACT_ALL            = YES

# If the EXTRACT_PRIVATE tag is set to YES all private members of a class
# will be included in the documentation.

EXTRACT_PRIVATE        = YES

# If the EXTRACT_PACKAGE tag is set to YES all members with package or internal
# scope will be included in the documentation.

EXTRACT_PACKAGE        = NO

# If the EXTRACT_STATIC tag is set to YES all static members of a file
# will be included in the documentation.

EXTRACT_STATIC
       = YES

# If the EXTRACT_LOCAL_CLASSES tag is set to YES classes (and structs)
# defined locally in source files will be included in the documentation.
# If set to NO only classes defined in header files are included.

EXTRACT_LOCAL_CLASSES  = YES

# This flag is only useful for Objective-C code. When set to YES local
# methods, which are defined in the implementation section but not in
# the interface are included in the documentation.
# If set to NO (the default) only methods in the interface are included.
```

```
EXTRACT_LOCAL_METHODS  = YES

# If this flag is set to YES, the members of anonymous namespaces will be
# extracted and appear in the documentation as a namespace called
# 'anonymous_namespace{file}', where file will be replaced with the base
# name of the file that contains the anonymous namespace. By default
# anonymous namespaces are hidden.

EXTRACT_ANON_NSPACES   = YES

# If the HIDE_UNDOC_MEMBERS tag is set to YES, Doxygen will hide all
# undocumented
 members of documented classes, files or namespaces.
# If set to NO (the default) these members will be included in the
# various overviews, but no documentation section is generated.
# This option has no effect if EXTRACT_ALL is enabled.

HIDE_UNDOC_MEMBERS     = NO

# If the HIDE_UNDOC_CLASSES tag is set to YES, Doxygen will hide all
# undocumented classes that are normally visible in the class hierarchy.
# If set to NO (the default) these classes will be included in the various
# overviews. This option has no effect if EXTRACT_ALL is enabled.

HIDE_UNDOC_CLASSES     = NO

# If the HIDE_FRIEND_COMPOUNDS tag is set to YES, Doxygen will hide all
# friend (class|struct|union) declarations.
# If set to NO (the default) these declarations will be included in the
# documentation.

HIDE_FRIEND_COMPOUNDS  = NO

# If the HIDE_IN_BODY_DOCS tag is set to YES, Doxygen will hide any
# documentation blocks found inside the body of a function.
# If set to NO (the default) these blocks will be appended
 to the
# function's detailed documentation block.

HIDE_IN_BODY_DOCS      = NO

# The INTERNAL_DOCS tag determines if documentation
# that is typed after a \internal command is included. If the tag is set
# to NO (the default) then the documentation will be excluded.
# Set it to YES to include the internal documentation.

INTERNAL_DOCS          = NO
```

```
# If the CASE_SENSE_NAMES tag is set to NO then Doxygen will only generate
# file names in lower-case letters. If set to YES upper-case letters are also
# allowed. This is useful if you have classes or files whose names only differ
# in case and if your file system supports case sensitive file names. Windows
# and Mac users are advised to set this option to NO.

CASE_SENSE_NAMES       = NO

# If the HIDE_SCOPE_NAMES tag is set to NO (the default) then Doxygen
# will show members with their full class and namespace scopes in the
# documentation. If set to YES the scope will be hidden.

HIDE_SCOPE_NAMES       = NO

# If the SHOW_INCLUDE_FILES
 tag is set to YES (the default) then Doxygen
# will put a list of the files that are included by a file in the documentation
# of that file.

SHOW_INCLUDE_FILES     = YES

# If the FORCE_LOCAL_INCLUDES tag is set to YES then Doxygen
# will list include files with double quotes in the documentation
# rather than with sharp brackets.

FORCE_LOCAL_INCLUDES   = NO

# If the INLINE_INFO tag is set to YES (the default) then a tag [inline]
# is inserted in the documentation for inline members.

INLINE_INFO            = YES

# If the SORT_MEMBER_DOCS tag is set to YES (the default) then doxygen
# will sort the (detailed) documentation of file and class members
# alphabetically by member name. If set to NO the members will appear in
# declaration order.

SORT_MEMBER_DOCS       = YES

# If the SORT_BRIEF_DOCS tag is set to YES then doxygen will sort the
# brief documentation of file, namespace and class members alphabetically
# by member name. If set to NO (the default) the members will
 appear in
# declaration order.

SORT_BRIEF_DOCS        = NO
```

```
# If the SORT_MEMBERS_CTORS_1ST tag is set to YES then doxygen
# will sort the (brief and detailed) documentation of class members so that
# constructors and destructors are listed first. If set to NO (the default)
# the constructors will appear in the respective orders defined by
# SORT_MEMBER_DOCS and SORT_BRIEF_DOCS.
# This tag will be ignored for brief docs if SORT_BRIEF_DOCS is set to NO
# and ignored for detailed docs if SORT_MEMBER_DOCS is set to NO.

SORT_MEMBERS_CTORS_1ST = NO

# If the SORT_GROUP_NAMES tag is set to YES then doxygen will sort the
# hierarchy of group names into alphabetical order. If set to NO (the default)
# the group names will appear in their defined order.

SORT_GROUP_NAMES       = NO

# If the SORT_BY_SCOPE_NAME tag is set to YES, the class list will be
# sorted by fully-qualified names, including namespaces. If set to
# NO (the default), the class list will be sorted only by class name,
# not
 including the namespace part.
# Note: This option is not very useful if HIDE_SCOPE_NAMES is set to YES.
# Note: This option applies only to the class list, not to the
# alphabetical list.

SORT_BY_SCOPE_NAME     = NO

# If the STRICT_PROTO_MATCHING option is enabled and doxygen fails to
# do proper type resolution of all parameters of a function it will reject a
# match between the prototype and the implementation of a member function even
# if there is only one candidate or it is obvious which candidate to choose
# by doing a simple string match. By disabling STRICT_PROTO_MATCHING doxygen
# will still accept a match between prototype and implementation in such cases.

STRICT_PROTO_MATCHING  = NO

# The GENERATE_TODOLIST tag can be used to enable (YES) or
# disable (NO) the todo list. This list is created by putting \todo
# commands in the documentation.

GENERATE_TODOLIST      = YES

# The GENERATE_TESTLIST tag can be used to enable (YES) or
# disable (NO) the test list. This list is
 created by putting \test
# commands in the documentation.

GENERATE_TESTLIST      = YES
```

```
# The GENERATE_BUGLIST tag can be used to enable (YES) or
# disable (NO) the bug list. This list is created by putting \bug
# commands in the documentation.

GENERATE_BUGLIST       = YES

# The GENERATE_DEPRECATEDLIST tag can be used to enable (YES) or
# disable (NO) the deprecated list. This list is created by putting
# \deprecated commands in the documentation.

GENERATE_DEPRECATEDLIST= YES

# The ENABLED_SECTIONS tag can be used to enable conditional
# documentation sections, marked by \if section-label ... \endif
# and \cond section-label ... \endcond blocks.

ENABLED_SECTIONS       =

# The MAX_INITIALIZER_LINES tag determines the maximum number of lines
# the initial value of a variable or macro consists of for it to appear in
# the documentation. If the initializer consists of more lines than specified
# here it will be hidden. Use a value of 0 to hide initializers completely.
# The appearance
 of the initializer of individual variables and macros in the
# documentation can be controlled using \showinitializer or \hideinitializer
# command in the documentation regardless of this setting.

MAX_INITIALIZER_LINES  = 30

# Set the SHOW_USED_FILES tag to NO to disable the list of files generated
# at the bottom of the documentation of classes and structs. If set to YES the
# list will mention the files that were used to generate the documentation.

SHOW_USED_FILES        = YES

# Set the SHOW_FILES tag to NO to disable the generation of the Files page.
# This will remove the Files entry from the Quick Index and from the
# Folder Tree View (if specified). The default is YES.

SHOW_FILES             = YES

# Set the SHOW_NAMESPACES tag to NO to disable the generation of the
# Namespaces page.
# This will remove the Namespaces entry from the Quick Index
# and from the Folder Tree View (if specified). The default is YES.

SHOW_NAMESPACES        = YES
```

```
# The FILE_VERSION_FILTER tag
 can be used to specify a program or script that
# doxygen should invoke to get the current version for each file (typically from
# the version control system). Doxygen will invoke the program by executing (via
# popen()) the command <command> <input-file>, where <command> is the value of
# the FILE_VERSION_FILTER tag, and <input-file> is the name of an input file
# provided by doxygen. Whatever the program writes to standard output
# is used as the file version. See the manual for examples.

FILE_VERSION_FILTER    =

# The LAYOUT_FILE tag can be used to specify a layout file which will be parsed
# by doxygen. The layout file controls the global structure of the generated
# output files in an output format independent way. To create the layout file
# that represents doxygen's defaults, run doxygen with the -l option.
# You can optionally specify a file name after the option, if omitted
# DoxygenLayout.xml will be used as the name of the layout file.

LAYOUT_FILE            =

# The CITE_BIB_FILES
 tag can be used to specify one or more bib files
# containing the references data. This must be a list of .bib files. The
# .bib extension is automatically appended if omitted. Using this command
# requires the bibtex tool to be installed. See also
# http://en.wikipedia.org/wiki/BibTeX for more info. For LaTeX the style
# of the bibliography can be controlled using LATEX_BIB_STYLE. To use this
# feature you need bibtex and perl available in the search path. Do not use
# file names with spaces, bibtex cannot handle them.

CITE_BIB_FILES         =

#---------------------------------------------------------------------------
# configuration options related to warning and progress messages
#---------------------------------------------------------------------------

# The QUIET tag can be used to turn on/off the messages that are generated
# by doxygen. Possible values are YES and NO. If left blank NO is used.

QUIET                  = NO

# The WARNINGS tag can be used to turn
 on/off the warning messages that are
# generated by doxygen. Possible values are YES and NO. If left blank
# NO is used.

WARNINGS               = YES
```

```
# If WARN_IF_UNDOCUMENTED is set to YES, then doxygen will generate warnings
# for undocumented members. If EXTRACT_ALL is set to YES then this flag will
# automatically be disabled.

WARN_IF_UNDOCUMENTED   = YES

# If WARN_IF_DOC_ERROR is set to YES, doxygen will generate warnings for
# potential errors in the documentation, such as not documenting some
# parameters in a documented function, or documenting parameters that
# don't exist or using markup commands wrongly.

WARN_IF_DOC_ERROR      = YES

# The WARN_NO_PARAMDOC option can be enabled to get warnings for
# functions that are documented, but have no documentation for their parameters
# or return value. If set to NO (the default) doxygen will only warn about
# wrong or incomplete parameter documentation, but not about the absence of
# documentation.

WARN_NO_PARAMDOC       = NO

#
 The WARN_FORMAT tag determines the format of the warning messages that
# doxygen can produce. The string should contain the $file, $line, and $text
# tags, which will be replaced by the file and line number from which the
# warning originated and the warning text. Optionally the format may contain
# $version, which will be replaced by the version of the file (if it could
# be obtained via FILE_VERSION_FILTER)

WARN_FORMAT            = "$file:$line: $text"

# The WARN_LOGFILE tag can be used to specify a file to which warning
# and error messages should be written. If left blank the output is written
# to stderr.

WARN_LOGFILE           =

#---------------------------------------------------------------------------
# configuration options related to the input files
#---------------------------------------------------------------------------

# The INPUT tag can be used to specify the files and/or directories that contain
# documented source files. You may enter file names like "myfile.cpp"
 or
# directories like "/usr/src/myproject". Separate the files or directories
# with spaces.
```

```
INPUT                  = .

# This tag can be used to specify the character encoding of the source files
# that doxygen parses. Internally doxygen uses the UTF-8 encoding, which is
# also the default input encoding. Doxygen uses libiconv (or the iconv built
# into libc) for the transcoding. See http://www.gnu.org/software/libiconv for
# the list of possible encodings.

INPUT_ENCODING         = UTF-8

# If the value of the INPUT tag contains directories, you can use the
# FILE_PATTERNS tag to specify one or more wildcard pattern (like *.cpp
# and *.h) to filter out the source-files in the directories. If left
# blank the following patterns are tested:
# *.c *.cc *.cxx *.cpp *.c++ *.d *.java *.ii *.ixx *.ipp *.i++ *.inl *.h *.hh
# *.hxx *.hpp *.h++ *.idl *.odl *.cs *.php *.php3 *.inc *.m *.mm *.dox *.py
# *.f90 *.f *.for *.vhd *.vhdl

FILE_PATTERNS          = *.h

# The RECURSIVE tag can
 be used to turn specify whether or not subdirectories
# should be searched for input files as well. Possible values are YES and NO.
# If left blank NO is used.

RECURSIVE              = YES

# The EXCLUDE tag can be used to specify files and/or directories that should be
# excluded from the INPUT source files. This way you can easily exclude a
# subdirectory from a directory tree whose root is specified with the INPUT tag.
# Note that relative paths are relative to the directory from which doxygen is
# run.

EXCLUDE                = configs yotta/module

# The EXCLUDE_SYMLINKS tag can be used to select whether or not files or
# directories that are symbolic links (a Unix file system feature) are excluded
# from the input.

EXCLUDE_SYMLINKS       = NO

# If the value of the INPUT tag contains directories, you can use the
# EXCLUDE_PATTERNS tag to specify one or more wildcard patterns to exclude
# certain files from those directories. Note that the wildcards are matched
# against the file
 with absolute path, so to exclude all test directories
# for example use the pattern */test/*
```

```
EXCLUDE_PATTERNS       = *_internal.h *_wrap.h

# The EXCLUDE_SYMBOLS tag can be used to specify one or more symbol names
# (namespaces, classes, functions, etc.) that should be excluded from the
# output. The symbol name can be a fully qualified name, a word, or if the
# wildcard * is used, a substring. Examples: ANamespace, AClass,
# AClass::ANamespace, ANamespace::*Test

EXCLUDE_SYMBOLS        =

# The EXAMPLE_PATH tag can be used to specify one or more files or
# directories that contain example code fragments that are included (see
# the \include command).

EXAMPLE_PATH           =

# If the value of the EXAMPLE_PATH tag contains directories, you can use the
# EXAMPLE_PATTERNS tag to specify one or more wildcard pattern (like *.cpp
# and *.h) to filter out the source-files in the directories. If left
# blank all files are included.

EXAMPLE_PATTERNS       = *

# If the EXAMPLE_RECURSIVE
 tag is set to YES then subdirectories will be
# searched for input files to be used with the \include or \dontinclude
# commands irrespective of the value of the RECURSIVE tag.
# Possible values are YES and NO. If left blank NO is used.

EXAMPLE_RECURSIVE      = NO

# The IMAGE_PATH tag can be used to specify one or more files or
# directories that contain image that are included in the documentation (see
# the \image command).

IMAGE_PATH             =

# The INPUT_FILTER tag can be used to specify a program that doxygen should
# invoke to filter for each input file. Doxygen will invoke the filter program
# by executing (via popen()) the command <filter> <input-file>, where <filter>
# is the value of the INPUT_FILTER tag, and <input-file> is the name of an
# input file. Doxygen will then use the output that the filter program writes
# to standard output.
# If FILTER_PATTERNS is specified, this tag will be ignored.
# Note that the filter must not add or remove lines; it is applied before
 the
# code is scanned, but not when the output code is generated. If lines are added
# or removed, the anchors will not be placed correctly.
```

```
INPUT_FILTER           =

# The FILTER_PATTERNS tag can be used to specify filters on a per file pattern
# basis.
# Doxygen will compare the file name with each pattern and apply the
# filter if there is a match.
# The filters are a list of the form:
# pattern=filter (like *.cpp=my_cpp_filter). See INPUT_FILTER for further
# info on how filters are used. If FILTER_PATTERNS is empty or if
# non of the patterns match the file name, INPUT_FILTER is applied.

FILTER_PATTERNS        =

# If the FILTER_SOURCE_FILES tag is set to YES, the input filter (if set using
# INPUT_FILTER) will be used to filter the input files when producing source
# files to browse (i.e. when SOURCE_BROWSER is set to YES).

FILTER_SOURCE_FILES    = NO

# The FILTER_SOURCE_PATTERNS tag can be used to specify source filters per file
# pattern. A pattern will override the setting
 for FILTER_PATTERN (if any)
# and it is also possible to disable source filtering for a specific pattern
# using *.ext= (so without naming a filter). This option only has effect when
# FILTER_SOURCE_FILES is enabled.

FILTER_SOURCE_PATTERNS =

# If the USE_MD_FILE_AS_MAINPAGE tag refers to the name of a markdown file that
# is part of the input, its contents will be placed on the main page
# (index.html). This can be useful if you have a project on for instance GitHub
# and want reuse the introduction page also for the doxygen output.

USE_MDFILE_AS_MAINPAGE =

#---------------------------------------------------------------------------
# configuration options related to source browsing
#---------------------------------------------------------------------------

# If the SOURCE_BROWSER tag is set to YES then a list of source files will
# be generated. Documented entities will be cross-referenced with these sources.
# Note: To get rid of all source code in the generated output, make
 sure also
# VERBATIM_HEADERS is set to NO.

SOURCE_BROWSER         = YES
```

```
# Setting the INLINE_SOURCES tag to YES will include the body
# of functions and classes directly in the documentation.

INLINE_SOURCES         = NO

# Setting the STRIP_CODE_COMMENTS tag to YES (the default) will instruct
# doxygen to hide any special comment blocks from generated source code
# fragments. Normal C, C++ and Fortran comments will always remain visible.

STRIP_CODE_COMMENTS    = YES

# If the REFERENCED_BY_RELATION tag is set to YES
# then for each documented function all documented
# functions referencing it will be listed.

REFERENCED_BY_RELATION = YES

# If the REFERENCES_RELATION tag is set to YES
# then for each documented function all documented entities
# called/used by that function will be listed.

REFERENCES_RELATION    = YES

# If the REFERENCES_LINK_SOURCE tag is set to YES (the default)
# and SOURCE_BROWSER tag is set to YES, then the hyperlinks from
# functions in REFERENCES_RELATION
 and REFERENCED_BY_RELATION lists will
# link to the source code.
# Otherwise they will link to the documentation.

REFERENCES_LINK_SOURCE = YES

# If the USE_HTAGS tag is set to YES then the references to source code
# will point to the HTML generated by the htags(1) tool instead of doxygen
# built-in source browser. The htags tool is part of GNU's global source
# tagging system (see http://www.gnu.org/software/global/global.html). You
# will need version 4.8.6 or higher.

USE_HTAGS              = NO

# If the VERBATIM_HEADERS tag is set to YES (the default) then Doxygen
# will generate a verbatim copy of the header file for each class for
# which an include is specified. Set to NO to disable this.

VERBATIM_HEADERS       = YES

#---------------------------------------------------------------------------
# configuration options related to the alphabetical class index
```

```
#---------------------------------------------------------------------------

# If the ALPHABETICAL_INDEX tag is set
 to YES, an alphabetical index
# of all compounds will be generated. Enable this if the project
# contains a lot of classes, structs, unions or interfaces.

ALPHABETICAL_INDEX     = NO

# If the alphabetical index is enabled (see ALPHABETICAL_INDEX) then
# the COLS_IN_ALPHA_INDEX tag can be used to specify the number of columns
# in which this list will be split (can be a number in the range [1..20])

COLS_IN_ALPHA_INDEX    = 5

# In case all classes in a project start with a common prefix, all
# classes will be put under the same header in the alphabetical index.
# The IGNORE_PREFIX tag can be used to specify one or more prefixes that
# should be ignored while generating the index headers.

IGNORE_PREFIX          =

#---------------------------------------------------------------------------
# configuration options related to the HTML output
#---------------------------------------------------------------------------

# If the GENERATE_HTML tag is set to YES (the default) Doxygen will
#
 generate HTML output.

GENERATE_HTML          = YES

# The HTML_OUTPUT tag is used to specify where the HTML docs will be put.
# If a relative path is entered the value of OUTPUT_DIRECTORY will be
# put in front of it. If left blank `html' will be used as the default path.

HTML_OUTPUT            = .

# The HTML_FILE_EXTENSION tag can be used to specify the file extension for
# each generated HTML page (for example: .htm,.php,.asp). If it is left blank
# doxygen will generate files with .html extension.

HTML_FILE_EXTENSION    = .html

# The HTML_HEADER tag can be used to specify a personal HTML header for
# each generated HTML page. If it is left blank doxygen will generate a
# standard header. Note that when using a custom header you are responsible
#  for the proper inclusion of any scripts and style sheets that doxygen
```

```
# needs, which is dependent on the configuration options used.
# It is advised to generate a default header using "doxygen -w html
# header.html footer.html stylesheet.css
 YourConfigFile" and then modify
# that header. Note that the header is subject to change so you typically
# have to redo this when upgrading to a newer version of doxygen or when
# changing the value of configuration settings such as GENERATE_TREEVIEW!

HTML_HEADER            =

# The HTML_FOOTER tag can be used to specify a personal HTML footer for
# each generated HTML page. If it is left blank doxygen will generate a
# standard footer.

HTML_FOOTER            =

# The HTML_STYLESHEET tag can be used to specify a user-defined cascading
# style sheet that is used by each HTML page. It can be used to
# fine-tune the look of the HTML output. If left blank doxygen will
# generate a default style sheet. Note that it is recommended to use
# HTML_EXTRA_STYLESHEET instead of this one, as it is more robust and this
# tag will in the future become obsolete.

HTML_STYLESHEET        =

# The HTML_EXTRA_STYLESHEET tag can be used to specify an additional
# user-defined cascading style sheet
 that is included after the standard
# style sheets created by doxygen. Using this option one can overrule
# certain style aspects. This is preferred over using HTML_STYLESHEET
# since it does not replace the standard style sheet and is therefor more
# robust against future updates. Doxygen will copy the style sheet file to
# the output directory.

HTML_EXTRA_STYLESHEET  =

# The HTML_EXTRA_FILES tag can be used to specify one or more extra images or
# other source files which should be copied to the HTML output directory. Note
# that these files will be copied to the base HTML output directory. Use the
# $relpath^ marker in the HTML_HEADER and/or HTML_FOOTER files to load these
# files. In the HTML_STYLESHEET file, use the file name only. Also note that
# the files will be copied as-is; there are no commands or markers available.

HTML_EXTRA_FILES       =

# The HTML_COLORSTYLE_HUE tag controls the color of the HTML output.
# Doxygen will adjust the colors in the style sheet and background
```

images
according to this color. Hue is specified as an angle on a colorwheel,
see http://en.wikipedia.org/wiki/Hue for more information.
For instance the value 0 represents red, 60 is yellow, 120 is green,
180 is cyan, 240 is blue, 300 purple, and 360 is red again.
The allowed range is 0 to 359.

HTML_COLORSTYLE_HUE   = 220

The HTML_COLORSTYLE_SAT tag controls the purity (or saturation) of
the colors in the HTML output. For a value of 0 the output will use
grayscales only. A value of 255 will produce the most vivid colors.

HTML_COLORSTYLE_SAT   = 100

The HTML_COLORSTYLE_GAMMA tag controls the gamma correction applied to
the luminance component of the colors in the HTML output. Values below
100 gradually make the output lighter, whereas values above 100 make
the output darker. The value divided by 100 is the actual gamma applied,
so 80 represents a gamma of 0.8, The value 220 represents a gamma of 2.2,
and 100 does not change the gamma.

HTML_COLORSTYLE_GAMMA
 = 80

If the HTML_TIMESTAMP tag is set to YES then the footer of each generated HTML
page will contain the date and time when the page was generated. Setting
this to NO can help when comparing the output of multiple runs.

HTML_TIMESTAMP   = YES

If the HTML_DYNAMIC_SECTIONS tag is set to YES then the generated HTML
documentation will contain sections that can be hidden and shown after the
page has loaded.

HTML_DYNAMIC_SECTIONS = NO

With HTML_INDEX_NUM_ENTRIES one can control the preferred number of
entries shown in the various tree structured indices initially; the user
can expand and collapse entries dynamically later on. Doxygen will expand
the tree to such a level that at most the specified number of entries are
visible (unless a fully collapsed tree already exceeds this amount).
So setting the number of entries 1 will produce a full collapsed tree by
default. 0 is a special value representing an infinite number of entries
and will
 result in a full expanded tree by default.

HTML_INDEX_NUM_ENTRIES = 100

```
# If the GENERATE_DOCSET tag is set to YES, additional index files
# will be generated that can be used as input for Apple's Xcode 3
# integrated development environment, introduced with OSX 10.5 (Leopard).
# To create a documentation set, doxygen will generate a Makefile in the
# HTML output directory. Running make will produce the docset in that
# directory and running "make install" will install the docset in
# ~/Library/Developer/Shared/Documentation/DocSets so that Xcode will find
# it at startup.
# See http://developer.apple.com/tools/creatingdocsetswithdoxygen.html
# for more information.

GENERATE_DOCSET        = NO

# When GENERATE_DOCSET tag is set to YES, this tag determines the name of the
# feed. A documentation feed provides an umbrella under which multiple
# documentation sets from a single provider (such as a company or product suite)
# can be grouped.

DOCSET_FEEDNAME        = "Doxygen generated
 docs"

# When GENERATE_DOCSET tag is set to YES, this tag specifies a string that
# should uniquely identify the documentation set bundle. This should be a
# reverse domain-name style string, e.g. com.mycompany.MyDocSet. Doxygen
# will append .docset to the name.

DOCSET_BUNDLE_ID       = org.doxygen.Project

# When GENERATE_PUBLISHER_ID tag specifies a string that should uniquely
# identify the documentation publisher. This should be a reverse domain-name
# style string, e.g. com.mycompany.MyDocSet.documentation.

DOCSET_PUBLISHER_ID    = org.doxygen.Publisher

# The GENERATE_PUBLISHER_NAME tag identifies the documentation publisher.

DOCSET_PUBLISHER_NAME  = Publisher

# If the GENERATE_HTMLHELP tag is set to YES, additional index files
# will be generated that can be used as input for tools like the
# Microsoft HTML help workshop to generate a compiled HTML help file (.chm)
# of the generated HTML documentation.

GENERATE_HTMLHELP      = NO

# If the GENERATE_HTMLHELP tag is set
```

```
 to YES, the CHM_FILE tag can
# be used to specify the file name of the resulting .chm file. You
# can add a path in front of the file if the result should not be
# written to the html output directory.

CHM_FILE               =

# If the GENERATE_HTMLHELP tag is set to YES, the HHC_LOCATION tag can
# be used to specify the location (absolute path including file name) of
# the HTML help compiler (hhc.exe). If non-empty doxygen will try to run
# the HTML help compiler on the generated index.hhp.

HHC_LOCATION           =

# If the GENERATE_HTMLHELP tag is set to YES, the GENERATE_CHI flag
# controls if a separate .chi index file is generated (YES) or that
# it should be included in the master .chm file (NO).

GENERATE_CHI           = NO

# If the GENERATE_HTMLHELP tag is set to YES, the CHM_INDEX_ENCODING
# is used to encode HtmlHelp index (hhk), content (hhc) and project file
# content.

CHM_INDEX_ENCODING     =

# If the GENERATE_HTMLHELP tag is set to YES, the BINARY_TOC flag
# controls
 whether a binary table of contents is generated (YES) or a
# normal table of contents (NO) in the .chm file.

BINARY_TOC             = NO

# The TOC_EXPAND flag can be set to YES to add extra items for group members
# to the contents of the HTML help documentation and to the tree view.

TOC_EXPAND             = NO

# If the GENERATE_QHP tag is set to YES and both QHP_NAMESPACE and
# QHP_VIRTUAL_FOLDER are set, an additional index file will be generated
# that can be used as input for Qt's qhelpgenerator to generate a
# Qt Compressed Help (.qch) of the generated HTML documentation.

GENERATE_QHP           = NO

# If the QHG_LOCATION tag is specified, the QCH_FILE tag can
# be used to specify the file name of the resulting .qch file.
# The path specified is relative to the HTML output folder.
```

```
QCH_FILE               =

# The QHP_NAMESPACE tag specifies the namespace to use when generating
# Qt Help Project output. For more information please see
# http://doc.trolltech.com/qthelpproject.html#namespace

QHP_NAMESPACE
        = org.doxygen.Project

# The QHP_VIRTUAL_FOLDER tag specifies the namespace to use when generating
# Qt Help Project output. For more information please see
# http://doc.trolltech.com/qthelpproject.html#virtual-folders

QHP_VIRTUAL_FOLDER     = doc

# If QHP_CUST_FILTER_NAME is set, it specifies the name of a custom filter to
# add. For more information please see
# http://doc.trolltech.com/qthelpproject.html#custom-filters

QHP_CUST_FILTER_NAME   =

# The QHP_CUST_FILT_ATTRS tag specifies the list of the attributes of the
# custom filter to add. For more information please see
# <a href="http://doc.trolltech.com/qthelpproject.html#custom-filters">
# Qt Help Project / Custom Filters</a>.

QHP_CUST_FILTER_ATTRS  =

# The QHP_SECT_FILTER_ATTRS tag specifies the list of the attributes this
# project's
# filter section matches.
# <a href="http://doc.trolltech.com/qthelpproject.html#filter-attributes">
# Qt Help Project / Filter Attributes</a>.

QHP_SECT_FILTER_ATTRS
  =

# If the GENERATE_QHP tag is set to YES, the QHG_LOCATION tag can
# be used to specify the location of Qt's qhelpgenerator.
# If non-empty doxygen will try to run qhelpgenerator on the generated
# .qhp file.

QHG_LOCATION           =

# If the GENERATE_ECLIPSEHELP tag is set to YES, additional index files
#  will be generated, which together with the HTML files, form an Eclipse help
# plugin. To install this plugin and make it available under the help contents
```

```
# menu in Eclipse, the contents of the directory containing the HTML and XML
# files needs to be copied into the plugins directory of eclipse. The name of
# the directory within the plugins directory should be the same as
# the ECLIPSE_DOC_ID value. After copying Eclipse needs to be restarted before
# the help appears.

GENERATE_ECLIPSEHELP   = NO

# A unique identifier for the eclipse help plugin. When installing the plugin
# the directory name containing the HTML and XML files should also have
# this name.

ECLIPSE_DOC_ID
       = org.doxygen.Project

# The DISABLE_INDEX tag can be used to turn on/off the condensed index (tabs)
# at top of each HTML page. The value NO (the default) enables the index and
# the value YES disables it. Since the tabs have the same information as the
# navigation tree you can set this option to NO if you already set
# GENERATE_TREEVIEW to YES.

DISABLE_INDEX          = NO

# The GENERATE_TREEVIEW tag is used to specify whether a tree-like index
# structure should be generated to display hierarchical information.
# If the tag value is set to YES, a side panel will be generated
# containing a tree-like index structure (just like the one that
# is generated for HTML Help). For this to work a browser that supports
# JavaScript, DHTML, CSS and frames is required (i.e. any modern browser).
# Windows users are probably better off using the HTML help feature.
# Since the tree basically has the same information as the tab index you
# could consider to set DISABLE_INDEX
 to NO when enabling this option.

GENERATE_TREEVIEW      = NO

# The ENUM_VALUES_PER_LINE tag can be used to set the number of enum values
# (range [0,1..20]) that doxygen will group on one line in the generated HTML
# documentation. Note that a value of 0 will completely suppress the enum
# values from appearing in the overview section.

ENUM_VALUES_PER_LINE   = 4

# If the treeview is enabled (see GENERATE_TREEVIEW) then this tag can be
# used to set the initial width (in pixels) of the frame in which the tree
# is shown.

TREEVIEW_WIDTH         = 250
```

```
# When the EXT_LINKS_IN_WINDOW option is set to YES doxygen will open
# links to external symbols imported via tag files in a separate window.

EXT_LINKS_IN_WINDOW    = NO

# Use this tag to change the font size of Latex formulas included
# as images in the HTML documentation. The default is 10. Note that
# when you change the font size after a successful doxygen run you need
# to manually remove any form_*.png images from the HTML
 output directory
# to force them to be regenerated.

FORMULA_FONTSIZE       = 10

# Use the FORMULA_TRANPARENT tag to determine whether or not the images
# generated for formulas are transparent PNGs. Transparent PNGs are
# not supported properly for IE 6.0, but are supported on all modern browsers.
# Note that when changing this option you need to delete any form_*.png files
# in the HTML output before the changes have effect.

FORMULA_TRANSPARENT    = YES

# Enable the USE_MATHJAX option to render LaTeX formulas using MathJax
# (see http://www.mathjax.org) which uses client side Javascript for the
# rendering instead of using prerendered bitmaps. Use this if you do not
# have LaTeX installed or if you want to formulas look prettier in the HTML
# output. When enabled you may also need to install MathJax separately and
# configure the path to it using the MATHJAX_RELPATH option.

USE_MATHJAX            = NO

# When MathJax is enabled you can set the default output format to be used for
#
 the MathJax output. Supported types are HTML-CSS, NativeMML (i.e. MathML) and
# SVG. The default value is HTML-CSS, which is slower, but has the best
# compatibility.

MATHJAX_FORMAT         = HTML-CSS

# When MathJax is enabled you need to specify the location relative to the
# HTML output directory using the MATHJAX_RELPATH option. The destination
# directory should contain the MathJax.js script. For instance, if the mathjax
# directory is located at the same level as the HTML output directory, then
# MATHJAX_RELPATH should be ../mathjax. The default value points to
# the MathJax Content Delivery Network so you can quickly see the result without
# installing MathJax.
# However, it is strongly recommended to install a local
```

```
# copy of MathJax from http://www.mathjax.org before deployment.

MATHJAX_RELPATH        = http://cdn.mathjax.org/mathjax/latest

# The MATHJAX_EXTENSIONS tag can be used to specify one or MathJax extension
# names that should be enabled during MathJax rendering.

MATHJAX_EXTENSIONS
    =

# The MATHJAX_CODEFILE tag can be used to specify a file with javascript
# pieces of code that will be used on startup of the MathJax code.

MATHJAX_CODEFILE       =

# When the SEARCHENGINE tag is enabled doxygen will generate a search box
# for the HTML output. The underlying search engine uses javascript
# and DHTML and should work on any modern browser. Note that when using
# HTML help (GENERATE_HTMLHELP), Qt help (GENERATE_QHP), or docsets
# (GENERATE_DOCSET) there is already a search function so this one should
# typically be disabled. For large projects the javascript based search engine
# can be slow, then enabling SERVER_BASED_SEARCH may provide a better solution.

SEARCHENGINE           = NO

# When the SERVER_BASED_SEARCH tag is enabled the search engine will be
# implemented using a web server instead of a web client using Javascript.
# There are two flavours of web server based search depending on the
# EXTERNAL_SEARCH setting. When disabled,
 doxygen will generate a PHP script for
# searching and an index file used by the script. When EXTERNAL_SEARCH is
# enabled the indexing and searching needs to be provided by external tools.
# See the manual for details.

SERVER_BASED_SEARCH    = NO

# When EXTERNAL_SEARCH is enabled doxygen will no longer generate the PHP
# script for searching. Instead the search results are written to an XML file
# which needs to be processed by an external indexer. Doxygen will invoke an
# external search engine pointed to by the SEARCHENGINE_URL option to obtain
# the search results. Doxygen ships with an example indexer (doxyindexer) and
# search engine (doxysearch.cgi) which are based on the open source search
# engine library Xapian. See the manual for configuration details.

EXTERNAL_SEARCH        = NO

# The SEARCHENGINE_URL should point to a search engine hosted by a web server
# which will returned the search results when EXTERNAL_SEARCH is enabled.
```

```
# Doxygen ships with an example search engine
 (doxysearch) which is based on
# the open source search engine library Xapian. See the manual for configuration
# details.

SEARCHENGINE_URL       =

# When SERVER_BASED_SEARCH and EXTERNAL_SEARCH are both enabled the unindexed
# search data is written to a file for indexing by an external tool. With the
# SEARCHDATA_FILE tag the name of this file can be specified.

SEARCHDATA_FILE        = searchdata.xml

# When SERVER_BASED_SEARCH AND EXTERNAL_SEARCH are both enabled the
# EXTERNAL_SEARCH_ID tag can be used as an identifier for the project. This is
# useful in combination with EXTRA_SEARCH_MAPPINGS to search through multiple
# projects and redirect the results back to the right project.

EXTERNAL_SEARCH_ID     =

# The EXTRA_SEARCH_MAPPINGS tag can be used to enable searching through doxygen
# projects other than the one defined by this configuration file, but that are
# all added to the same external search index. Each project needs to have a
# unique id set via EXTERNAL_SEARCH_ID.
 The search mapping then maps the id
# of to a relative location where the documentation can be found.
# The format is: EXTRA_SEARCH_MAPPINGS = id1=loc1 id2=loc2 ...

EXTRA_SEARCH_MAPPINGS  =

#---------------------------------------------------------------------------
# configuration options related to the LaTeX output
#---------------------------------------------------------------------------

# If the GENERATE_LATEX tag is set to YES (the default) Doxygen will
# generate Latex output.

GENERATE_LATEX         = NO

# The LATEX_OUTPUT tag is used to specify where the LaTeX docs will be put.
# If a relative path is entered the value of OUTPUT_DIRECTORY will be
# put in front of it. If left blank `latex' will be used as the default path.

LATEX_OUTPUT           = latex

# The LATEX_CMD_NAME tag can be used to specify the LaTeX command name to be
# invoked. If left blank `latex' will be used as the default command name.
# Note that when enabling USE_PDFLATEX this option is only used
```

```
 for
# generating bitmaps for formulas in the HTML output, but not in the
# Makefile that is written to the output directory.

LATEX_CMD_NAME         = latex

# The MAKEINDEX_CMD_NAME tag can be used to specify the command name to
# generate index for LaTeX. If left blank `makeindex' will be used as the
# default command name.

MAKEINDEX_CMD_NAME     = makeindex

# If the COMPACT_LATEX tag is set to YES Doxygen generates more compact
# LaTeX documents. This may be useful for small projects and may help to
# save some trees in general.

COMPACT_LATEX          = YES

# The PAPER_TYPE tag can be used to set the paper type that is used
# by the printer. Possible values are: a4, letter, legal and
# executive. If left blank a4 will be used.

PAPER_TYPE             = a4wide

# The EXTRA_PACKAGES tag can be to specify one or more names of LaTeX
# packages that should be included in the LaTeX output.

EXTRA_PACKAGES         =

# The LATEX_HEADER tag can be used to specify a personal LaTeX header
 for
# the generated latex document. The header should contain everything until
# the first chapter. If it is left blank doxygen will generate a
# standard header. Notice: only use this tag if you know what you are doing!

LATEX_HEADER           =

# The LATEX_FOOTER tag can be used to specify a personal LaTeX footer for
# the generated latex document. The footer should contain everything after
# the last chapter. If it is left blank doxygen will generate a
# standard footer. Notice: only use this tag if you know what you are doing!

LATEX_FOOTER           =

# The LATEX_EXTRA_FILES tag can be used to specify one or more extra images
# or other source files which should be copied to the LaTeX output directory.
# Note that the files will be copied as-is; there are no commands or markers
# available.
```

```
LATEX_EXTRA_FILES      =

# If the PDF_HYPERLINKS tag is set to YES, the LaTeX that is generated
# is prepared for conversion to pdf (using ps2pdf). The pdf file will
# contain links (just
 like the HTML output) instead of page references
# This makes the output suitable for online browsing using a pdf viewer.

PDF_HYPERLINKS         = YES

# If the USE_PDFLATEX tag is set to YES, pdflatex will be used instead of
# plain latex in the generated Makefile. Set this option to YES to get a
# higher quality PDF documentation.

USE_PDFLATEX           = YES

# If the LATEX_BATCHMODE tag is set to YES, doxygen will add the \\batchmode.
# command to the generated LaTeX files. This will instruct LaTeX to keep
# running if errors occur, instead of asking the user for help.
# This option is also used when generating formulas in HTML.

LATEX_BATCHMODE        = NO

# If LATEX_HIDE_INDICES is set to YES then doxygen will not
# include the index chapters (such as File Index, Compound Index, etc.)
# in the output.

LATEX_HIDE_INDICES     = NO

# If LATEX_SOURCE_CODE is set to YES then doxygen will include
# source code with syntax highlighting in the LaTeX output.
# Note that which sources
 are shown also depends on other settings
# such as SOURCE_BROWSER.

LATEX_SOURCE_CODE      = NO

# The LATEX_BIB_STYLE tag can be used to specify the style to use for the
# bibliography, e.g. plainnat, or ieeetr. The default style is "plain". See
# http://en.wikipedia.org/wiki/BibTeX for more info.

LATEX_BIB_STYLE        = plain

#---------------------------------------------------------------------------
# configuration options related to the RTF output
#---------------------------------------------------------------------------
```

```
# If the GENERATE_RTF tag is set to YES Doxygen will generate RTF output
# The RTF output is optimized for Word 97 and may not look very pretty with
# other RTF readers or editors.

GENERATE_RTF           = NO

# The RTF_OUTPUT tag is used to specify where the RTF docs will be put.
# If a relative path is entered the value of OUTPUT_DIRECTORY will be
# put in front of it. If left blank `rtf' will be used as the default path.

RTF_OUTPUT             = rtf

#
 If the COMPACT_RTF tag is set to YES Doxygen generates more compact
# RTF documents. This may be useful for small projects and may help to
# save some trees in general.

COMPACT_RTF            = NO

# If the RTF_HYPERLINKS tag is set to YES, the RTF that is generated
# will contain hyperlink fields. The RTF file will
# contain links (just like the HTML output) instead of page references.
# This makes the output suitable for online browsing using WORD or other
# programs which support those fields.
# Note: wordpad (write) and others do not support links.

RTF_HYPERLINKS         = NO

# Load style sheet definitions from file. Syntax is similar to doxygen's
# config file, i.e. a series of assignments. You only have to provide
# replacements, missing definitions are set to their default value.

RTF_STYLESHEET_FILE    =

# Set optional variables used in the generation of an rtf document.
# Syntax is similar to doxygen's config file.

RTF_EXTENSIONS_FILE    =

#---------------------------------------------------------------------------
#
 configuration options related to the man page output
#---------------------------------------------------------------------------

# If the GENERATE_MAN tag is set to YES (the default) Doxygen will
# generate man pages

GENERATE_MAN           = NO
```

```
# The MAN_OUTPUT tag is used to specify where the man pages will be put.
# If a relative path is entered the value of OUTPUT_DIRECTORY will be
# put in front of it. If left blank `man' will be used as the default path.

MAN_OUTPUT             = man

# The MAN_EXTENSION tag determines the extension that is added to
# the generated man pages (default is the subroutine's section .3)

MAN_EXTENSION          = .3

# If the MAN_LINKS tag is set to YES and Doxygen generates man output,
# then it will generate one additional man file for each entity
# documented in the real man page(s). These additional files
# only source the real man page, but without them the man command
# would be unable to find
 the correct page. The default is NO.

MAN_LINKS              = NO

#---------------------------------------------------------------------------
# configuration options related to the XML output
#---------------------------------------------------------------------------

# If the GENERATE_XML tag is set to YES Doxygen will
# generate an XML file that captures the structure of
# the code including all documentation.

GENERATE_XML           = NO

# The XML_OUTPUT tag is used to specify where the XML pages will be put.
# If a relative path is entered the value of OUTPUT_DIRECTORY will be
# put in front of it. If left blank `xml' will be used as the default path.

XML_OUTPUT             = xml

# The XML_SCHEMA tag can be used to specify an XML schema,
# which can be used by a validating XML parser to check the
# syntax of the XML files.

#XML_SCHEMA             =

# The XML_DTD tag can be used to specify an XML DTD,
# which can be used by a validating XML parser to check the
# syntax of the
 XML files.
```

```
#XML_DTD            =

# If the XML_PROGRAMLISTING tag is set to YES Doxygen will
# dump the program listings (including syntax highlighting
# and cross-referencing information) to the XML output. Note that
# enabling this will significantly increase the size of the XML output.

XML_PROGRAMLISTING     = YES

#---------------------------------------------------------------------------
# configuration options related to the DOCBOOK output
#---------------------------------------------------------------------------

# If the GENERATE_DOCBOOK tag is set to YES Doxygen will generate DOCBOOK files
# that can be used to generate PDF.

GENERATE_DOCBOOK       = NO

# The DOCBOOK_OUTPUT tag is used to specify where the DOCBOOK pages will be put.
# If a relative path is entered the value of OUTPUT_DIRECTORY will be put in
# front of it. If left blank docbook will be used as the default path.

DOCBOOK_OUTPUT         = docbook

#---------------------------------------------------------------------------
#
 configuration options for the AutoGen Definitions output
#---------------------------------------------------------------------------

# If the GENERATE_AUTOGEN_DEF tag is set to YES Doxygen will
# generate an AutoGen Definitions (see autogen.sf.net) file
# that captures the structure of the code including all
# documentation. Note that this feature is still experimental
# and incomplete at the moment.

GENERATE_AUTOGEN_DEF   = NO

#---------------------------------------------------------------------------
# configuration options related to the Perl module output
#---------------------------------------------------------------------------

# If the GENERATE_PERLMOD tag is set to YES Doxygen will
# generate a Perl module file that captures the structure of
# the code including all documentation. Note that this
# feature is still experimental and incomplete at the
# moment.

GENERATE_PERLMOD       = NO
```

```
# If the PERLMOD_LATEX tag is set to YES Doxygen will generate
#
 the necessary Makefile rules, Perl scripts and LaTeX code to be able
# to generate PDF and DVI output from the Perl module output.

PERLMOD_LATEX          = NO

# If the PERLMOD_PRETTY tag is set to YES the Perl module output will be
# nicely formatted so it can be parsed by a human reader.
# This is useful
# if you want to understand what is going on.
# On the other hand, if this
# tag is set to NO the size of the Perl module output will be much smaller
# and Perl will parse it just the same.

PERLMOD_PRETTY         = YES

# The names of the make variables in the generated doxyrules.make file
# are prefixed with the string contained in PERLMOD_MAKEVAR_PREFIX.
# This is useful so different doxyrules.make files included by the same
# Makefile don't overwrite each other's variables.

PERLMOD_MAKEVAR_PREFIX =

#---------------------------------------------------------------------------
# Configuration options related to the preprocessor
#---------------------------------------------------------------------------

#
 If the ENABLE_PREPROCESSING tag is set to YES (the default) Doxygen will
# evaluate all C-preprocessor directives found in the sources and include
# files.

ENABLE_PREPROCESSING   = YES

# If the MACRO_EXPANSION tag is set to YES Doxygen will expand all macro
# names in the source code. If set to NO (the default) only conditional
# compilation will be performed. Macro expansion can be done in a controlled
# way by setting EXPAND_ONLY_PREDEF to YES.

MACRO_EXPANSION        = NO

# If the EXPAND_ONLY_PREDEF and MACRO_EXPANSION tags are both set to YES
# then the macro expansion is limited to the macros specified with the
# PREDEFINED and EXPAND_AS_DEFINED tags.

EXPAND_ONLY_PREDEF     = NO
```

```
# If the SEARCH_INCLUDES tag is set to YES (the default) the includes files
# pointed to by INCLUDE_PATH will be searched when a #include is found.

SEARCH_INCLUDES        = YES

# The INCLUDE_PATH tag can be used to specify one or more directories that
# contain include
 files that are not input files but should be processed by
# the preprocessor.

INCLUDE_PATH           =

# You can use the INCLUDE_FILE_PATTERNS tag to specify one or more wildcard
# patterns (like *.h and *.hpp) to filter out the header-files in the
# directories. If left blank, the patterns specified with FILE_PATTERNS will
# be used.

INCLUDE_FILE_PATTERNS  =

# The PREDEFINED tag can be used to specify one or more macro names that
# are defined before the preprocessor is started (similar to the -D option of
# gcc). The argument of the tag is a list of macros of the form: name
# or name=definition (no spaces). If the definition and the = are
# omitted =1 is assumed. To prevent a macro definition from being
# undefined via #undef or recursively expanded use the := operator
# instead of the = operator.

PREDEFINED             = WIN32 \
                         NTLM \
                         USE_LZO \
                         ENABLE_FRAGMENT \
                         P2MP \

                        P2MP_SERVER \
                         USE_CRYPTO \
                         USE_SSL \
                         ENABLE_PLUGIN \
                         ENABLE_MANAGEMENT \
                         ENABLE_OCC \
                         HAVE_GETTIMEOFDAY

# If the MACRO_EXPANSION and EXPAND_ONLY_PREDEF tags are set to YES then
# this tag can be used to specify a list of macro names that should be expanded.
# The macro definition that is found in the sources will be used.
# Use the PREDEFINED tag if you want to use a different macro definition that
# overrules the definition found in the source code.
```

```
EXPAND_AS_DEFINED      =

# If the SKIP_FUNCTION_MACROS tag is set to YES (the default) then
# doxygen's preprocessor will remove all references to function-like macros
# that are alone on a line, have an all uppercase name, and do not end with a
# semicolon, because these will confuse the parser if not removed.

SKIP_FUNCTION_MACROS   = YES

#---------------------------------------------------------------------------
#
 Configuration::additions related to external references
#---------------------------------------------------------------------------

# The TAGFILES option can be used to specify one or more tagfiles. For each
# tag file the location of the external documentation should be added. The
# format of a tag file without this location is as follows:
#
# TAGFILES = file1 file2 ...
# Adding location for the tag files is done as follows:
#
# TAGFILES = file1=loc1 "file2 = loc2" ...
# where "loc1" and "loc2" can be relative or absolute paths
# or URLs. Note that each tag file must have a unique name (where the name does
# NOT include the path). If a tag file is not located in the directory in which
# doxygen is run, you must also specify the path to the tagfile here.

TAGFILES               =

# When a file name is specified after GENERATE_TAGFILE, doxygen will create
# a tag file that is based on the input files it reads.

GENERATE_TAGFILE
  =

# If the ALLEXTERNALS tag is set to YES all external classes will be listed
# in the class index. If set to NO only the inherited external classes
# will be listed.

ALLEXTERNALS           = NO

# If the EXTERNAL_GROUPS tag is set to YES all external groups will be listed
# in the modules index. If set to NO, only the current project's groups will
# be listed.

EXTERNAL_GROUPS        = YES

# If the EXTERNAL_PAGES tag is set to YES all external pages will be listed
```

```
# in the related pages index. If set to NO, only the current project's
# pages will be listed.

EXTERNAL_PAGES        = YES

# The PERL_PATH should be the absolute path and name of the perl script
# interpreter (i.e. the result of `which perl').

PERL_PATH             = /usr/bin/perl

#---------------------------------------------------------------------------
# Configuration options related to the dot tool
#---------------------------------------------------------------------------

# If the CLASS_DIAGRAMS tag is set
 to YES (the default) Doxygen will
# generate a inheritance diagram (in HTML, RTF and LaTeX) for classes with base
# or super classes. Setting the tag to NO turns the diagrams off. Note that
# this option also works with HAVE_DOT disabled, but it is recommended to
# install and use dot, since it yields more powerful graphs.

CLASS_DIAGRAMS        = NO

# You can define message sequence charts within doxygen comments using the \msc
# command. Doxygen will then run the mscgen tool (see
# http://www.mcternan.me.uk/mscgen/) to produce the chart and insert it in the
# documentation. The MSCGEN_PATH tag allows you to specify the directory where
# the mscgen tool resides. If left empty the tool is assumed to be found in the
# default search path.

MSCGEN_PATH           =

# If set to YES, the inheritance and collaboration graphs will hide
# inheritance and usage relations if the target is undocumented
# or is not a class.

HIDE_UNDOC_RELATIONS   = YES

# If you set the HAVE_DOT tag to YES then
 doxygen will assume the dot tool is
# available from the path. This tool is part of Graphviz, a graph visualization
# toolkit from AT&T and Lucent Bell Labs. The other options in this section
# have no effect if this option is set to NO (the default)

HAVE_DOT              = YES

# The DOT_NUM_THREADS specifies the number of dot invocations doxygen is
# allowed to run in parallel. When set to 0 (the default) doxygen will
```

```
# base this on the number of processors available in the system. You can set it
# explicitly to a value larger than 0 to get control over the balance
# between CPU load and processing speed.

DOT_NUM_THREADS        = 0

# By default doxygen will use the Helvetica font for all dot files that
# doxygen generates. When you want a differently looking font you can specify
# the font name using DOT_FONTNAME. You need to make sure dot is able to find
# the font, which can be done by putting it in a standard location or by setting
# the DOTFONTPATH environment variable or
 by setting DOT_FONTPATH to the
# directory containing the font.

DOT_FONTNAME           = Helvetica

# The DOT_FONTSIZE tag can be used to set the size of the font of dot graphs.
# The default size is 10pt.

DOT_FONTSIZE           = 10

# By default doxygen will tell dot to use the Helvetica font.
# If you specify a different font using DOT_FONTNAME you can use DOT_FONTPATH to
# set the path where dot can find it.

DOT_FONTPATH           =

# If the CLASS_GRAPH and HAVE_DOT tags are set to YES then doxygen
# will generate a graph for each documented class showing the direct and
# indirect inheritance relations. Setting this tag to YES will force the
# CLASS_DIAGRAMS tag to NO.

CLASS_GRAPH            = YES

# If the COLLABORATION_GRAPH and HAVE_DOT tags are set to YES then doxygen
# will generate a graph for each documented class showing the direct and
# indirect implementation dependencies (inheritance, containment, and
# class references variables) of the class with other documented
 classes.

COLLABORATION_GRAPH    = YES

# If the GROUP_GRAPHS and HAVE_DOT tags are set to YES then doxygen
# will generate a graph for groups, showing the direct groups dependencies

GROUP_GRAPHS           = YES

# If the UML_LOOK tag is set to YES doxygen will generate inheritance and
```

```
# collaboration diagrams in a style similar to the OMG's Unified Modeling
# Language.

UML_LOOK               = NO

# If the UML_LOOK tag is enabled, the fields and methods are shown inside
# the class node. If there are many fields or methods and many nodes the
# graph may become too big to be useful. The UML_LIMIT_NUM_FIELDS
# threshold limits the number of items for each type to make the size more
# manageable. Set this to 0 for no limit. Note that the threshold may be
# exceeded by 50% before the limit is enforced.

UML_LIMIT_NUM_FIELDS   = 10

# If set to YES, the inheritance and collaboration graphs will show the
# relations between templates and their instances.

TEMPLATE_RELATIONS     = NO

# If
 the ENABLE_PREPROCESSING, SEARCH_INCLUDES, INCLUDE_GRAPH, and HAVE_DOT
# tags are set to YES then doxygen will generate a graph for each documented
# file showing the direct and indirect include dependencies of the file with
# other documented files.

INCLUDE_GRAPH          = YES

# If the ENABLE_PREPROCESSING, SEARCH_INCLUDES, INCLUDED_BY_GRAPH, and
# HAVE_DOT tags are set to YES then doxygen will generate a graph for each
# documented header file showing the documented files that directly or
# indirectly include this file.

INCLUDED_BY_GRAPH      = YES

# If the CALL_GRAPH and HAVE_DOT options are set to YES then
# doxygen will generate a call dependency graph for every global function
# or class method. Note that enabling this option will significantly increase
# the time of a run. So in most cases it will be better to enable call graphs
# for selected functions only using the \callgraph command.

CALL_GRAPH             = NO

# If the CALLER_GRAPH and HAVE_DOT tags are set to YES
 then
# doxygen will generate a caller dependency graph for every global function
# or class method. Note that enabling this option will significantly increase
# the time of a run. So in most cases it will be better to enable caller
# graphs for selected functions only using the \callergraph command.
```

```
CALLER_GRAPH          = NO

# If the GRAPHICAL_HIERARCHY and HAVE_DOT tags are set to YES then doxygen
# will generate a graphical hierarchy of all classes instead of a textual one.

GRAPHICAL_HIERARCHY    = YES

# If the DIRECTORY_GRAPH and HAVE_DOT tags are set to YES
# then doxygen will show the dependencies a directory has on other directories
# in a graphical way. The dependency relations are determined by the #include
# relations between the files in the directories.

DIRECTORY_GRAPH        = YES

# The DOT_IMAGE_FORMAT tag can be used to set the image format of the images
# generated by dot. Possible values are svg, png, jpg, or gif.
# If left blank png will be used. If you choose
 svg you need to set
# HTML_FILE_EXTENSION to xhtml in order to make the SVG files
# visible in IE 9+ (other browsers do not have this requirement).

DOT_IMAGE_FORMAT       = png

# If DOT_IMAGE_FORMAT is set to svg, then this option can be set to YES to
# enable generation of interactive SVG images that allow zooming and panning.
# Note that this requires a modern browser other than Internet Explorer.
# Tested and working are Firefox, Chrome, Safari, and Opera. For IE 9+ you
# need to set HTML_FILE_EXTENSION to xhtml in order to make the SVG files
# visible. Older versions of IE do not have SVG support.

INTERACTIVE_SVG        = NO

# The tag DOT_PATH can be used to specify the path where the dot tool can be
# found. If left blank, it is assumed the dot tool can be found in the path.

DOT_PATH               =

# The DOTFILE_DIRS tag can be used to specify one or more directories that
# contain dot files that are included in the documentation (see the
# \dotfile command).

DOTFILE_DIRS
        =

# The MSCFILE_DIRS tag can be used to specify one or more directories that
# contain msc files that are included in the documentation (see the
# \mscfile command).
```

```
MSCFILE_DIRS           =

# The DOT_GRAPH_MAX_NODES tag can be used to set the maximum number of
# nodes that will be shown in the graph. If the number of nodes in a graph
# becomes larger than this value, doxygen will truncate the graph, which is
# visualized by representing a node as a red box. Note that doxygen if the
# number of direct children of the root node in a graph is already larger than
# DOT_GRAPH_MAX_NODES then the graph will not be shown at all. Also note
# that the size of a graph can be further restricted by MAX_DOT_GRAPH_DEPTH.

DOT_GRAPH_MAX_NODES    = 200

# The MAX_DOT_GRAPH_DEPTH tag can be used to set the maximum depth of the
# graphs generated by dot. A depth value of 3 means that only nodes reachable
# from the root by following a path via at most 3 edges will be shown. Nodes
# that lay
 further from the root node will be omitted. Note that setting this
# option to 1 or 2 may greatly reduce the computation time needed for large
# code bases. Also note that the size of a graph can be further restricted by
# DOT_GRAPH_MAX_NODES. Using a depth of 0 means no depth restriction.

MAX_DOT_GRAPH_DEPTH    = 1000

# Set the DOT_TRANSPARENT tag to YES to generate images with a transparent
# background. This is disabled by default, because dot on Windows does not
# seem to support this out of the box. Warning: Depending on the platform used,
# enabling this option may lead to badly anti-aliased labels on the edges of
# a graph (i.e. they become hard to read).

DOT_TRANSPARENT        = YES

# Set the DOT_MULTI_TARGETS tag to YES allow dot to generate multiple output
# files in one run (i.e. multiple -o and -T options on the command line). This
# makes dot run faster, but since only newer versions of dot (>1.8.10)
# support this, this feature is disabled by default.

DOT_MULTI_TARGETS
     = NO

# If the GENERATE_LEGEND tag is set to YES (the default) Doxygen will
# generate a legend page explaining the meaning of the various boxes and
# arrows in the dot generated graphs.

GENERATE_LEGEND        = YES

# If the DOT_CLEANUP tag is set to YES (the default) Doxygen will
# remove the intermediate dot files that are used to generate
```

the various graphs.

DOT_CLEANUP = YES
README for mbed TLS
==========

Configuration
---

mbed TLS should build out of the box on most systems. Some platform specific options are available in the fully documented configuration file `include/mbedtls/config.h`, which is also the place where features can be selected. This file can be edited manually, or in a more programmatic way using the Perl script `scripts/config.pl` (use `--help` for usage instructions).

Compiler options can be set using conventional environment variables such as `CC` and `CFLAGS` when using the Make and CMake build system (see below).

Compiling

There are currently four active build systems used within mbed TLS releases:

- yotta
- Make
- CMake
- Microsoft Visual Studio (Visual Studio 6 and Visual Studio 2010)

The main systems used for development are CMake and Make. Those systems are always complete and up-to-date. The others should reflect all changes present in the CMake and Make build system, although features may not be ported there automatically.

Yotta, as a build system, is slightly different from the other build systems:

- it provides a minimalistic configuration file by default
- depending on the yotta target, features of mbed OS may be used in examples and tests

The Make and CMake build systems create three libraries: libmbedcrypto, libmbedx509, and libmbedtls. Note that libmbedtls depends on libmbedx509 and libmbedcrypto, and libmbedx509 depends on libmbedcrypto. As a result, some linkers will expect flags to be in a specific order, for example the GNU linker wants `-lmbedtls -lmbedx509 -lmbedcrypto`. Also, when loading shared libraries using dlopen(), you'll need to load libmbedcrypto first, then libmbedx509, before you can load libmbedtls.

Yotta

[yotta](http://yottabuild.org) is a package manager and build system developed by mbed, and is the build system of mbed OS 16.03. To install it on your platform, please follow the yotta [installation instructions](http://docs.yottabuild.org/#installing).

Once
yotta is installed, you can use it to download the latest version of mbed TLS from the yotta registry with:

```
yotta install mbedtls
```

and build it with:

```
yotta build
```

If, on the other hand, you already have a copy of mbed TLS from a source other than the yotta registry, for example from cloning our GitHub repository, or from downloading a tarball of the standalone edition, then you'll first need to generate the yotta module by running:

```
yotta/create-module.sh
```

This should be executed from the root mbed TLS project directory. This will create the yotta module in the `yotta/module` directory within it. You can then change to that directory and build as usual:

```
cd yotta/module
yotta build
```

In any case, you'll probably want to set the yotta target before building unless it has already been set globally. For more information on using yotta, please consult the [yotta documentation](http://docs.yottabuild.org/).

For more details on the yotta/mbed
OS edition of mbed TLS, including example programs, please consult the [Readme at the root of the yotta module](https://github.com/ARMmbed/mbedtls/blob/development/yotta/data/README.md).

Make

We intentionally only use the minimum of `Make` functionality, as a lot of `Make` features are not supported on all different implementations of Make or on different platforms. As such, the Makefiles sometimes require some manual changes or export statements in order to work for your platform.

In order to build from the source code using Make, just enter at the command line:

```
make
```

In order to run the tests, enter:

```
make check
```

The tests need Perl to be built and run. If you don't have Perl installed, you can skip building the tests with:

```
make no_test
```

You'll still be able to run a much smaller set of tests with:

```
programs/test/selftest
```

In order to build for a Windows platform, you should use `WINDOWS_BUILD=1` if the target is Windows but the build environment is Unix-like
(for instance when cross-compiling, or compiling from an MSYS shell), and `WINDOWS=1` if the build environment is a Windows shell (for instance using mingw32-make) (in that case some targets will not be available).

Setting the variable `SHARED` in your environment will build shared libraries in addition to the static libraries. Setting `DEBUG` gives you a debug build. You can override `CFLAGS` and `LDFLAGS` by setting them in your environment or on the make command line; if you do so, essential parts such as `-I` will still be preserved. Warning options may be overridden separately using `WARNING_CFLAGS`.

Depending on your platform, you might run into some issues. Please check the Makefiles in `library/`, `programs/` and `tests/` for options to manually add or remove for specific platforms. You can also check [the mbed TLS Knowledge Base](https://tls.mbed.org/kb) for articles on your platform or issue.

In case you find that you need to do something else as well, please let us
know what, so we can add it to the [mbed TLS knowledge base](https://tls.mbed.org/kb).

CMake

In order to build the source using CMake, just enter at the command line:

```
cmake .
make
```

In order to run the tests, enter:

```
make test
```

The test suites need Perl to be built. If you don't have Perl installed, you'll want to disable the test suites with:

```
cmake -DENABLE_TESTING=Off .
```

If you disabled the test suites, but kept the programs enabled, you can still run a much smaller set of tests with:

```
programs/test/selftest
```

To configure CMake for building shared libraries, use:

```
cmake -DUSE_SHARED_MBEDTLS_LIBRARY=On .
```

There are many different build modes available within the CMake buildsystem. Most of them are available for gcc and clang, though some are compiler-specific:

- Release. This generates the default code without any unnecessary information in the binary files.
- Debug. This generates debug information and disables optimization of the code.
- Coverage.

This generates code coverage information in addition to debug information.
- ASan. This instruments the code with AddressSanitizer to check for memory errors. (This includes LeakSanitizer, with recent version of gcc and clang.) (With recent version of clang, this mode also instruments the code with UndefinedSanitizer to check for undefined behaviour.)
- ASanDbg. Same as ASan but slower, with debug information and better stack traces.
- MemSan. This instruments the code with MemorySanitizer to check for uninitialised memory reads. Experimental, needs recent clang on Linux/x86_64.
- MemSanDbg. Same as MemSan but slower, with debug information, better stack traces and origin tracking.
- Check. This activates the compiler warnings that depend on optimization and treats all warnings as errors.

Switching build modes in CMake is simple. For debug mode, enter at the command line:

```
cmake -D CMAKE_BUILD_TYPE=Debug .
```

To list other available CMake options, use:

```
cmake -LH
```

Note
that, with CMake, if you want to change the compiler or its options after you already ran CMake, you need to clear its cache first, e.g. (using GNU find):

```
find . -iname '*cmake*' -not -name CMakeLists.txt -exec rm -rf {} +
CC=gcc CFLAGS='-fstack-protector-strong -Wa,--noexecstack' cmake .
```

Microsoft Visual Studio

The build files for Microsoft Visual Studio are generated for Visual Studio 2010.

The solution file `mbedTLS.sln` contains all the basic projects needed to build the library and all the programs. The files in tests are not generated and compiled, as these need a perl environment as well. However, the selftest program in `programs/test/` is still available.

Example programs

We've included example programs for a lot of different features and uses in `programs/`. Most programs only focus on a single feature or usage scenario, so keep that in mind when copying parts of the code.

Tests
---

mbed TLS includes an elaborate test suite in `tests/`
that initially requires Perl to generate the tests files (e.g. `test\_suite\_mpi.c`). These files are generated from a `function file` (e.g. `suites/test\_suite\_mpi.function`) and a `data file` (e.g. `suites/test\_suite\_mpi.data`). The `function file` contains the test functions. The `data file` contains the test cases, specified as parameters that will be passed to the test function.

For machines with a Unix shell and OpenSSL (and optionally GnuTLS) installed, additional test scripts are available:

- `tests/ssl-opt.sh` runs integration tests for various TLS options (renegotiation, resumption, etc.) and tests interoperability of these options with other implementations.
- `tests/compat.sh` tests interoperability of every ciphersuite with other implementations.
- `tests/scripts/test-ref-configs.pl` test builds in various reduced configurations.
- `tests/scripts/key-exchanges.pl` test builds in configurations with a single key exchange enabled
- `tests/scripts/all.sh` runs
 a combination of the above tests, plus some more, with various build options (such as ASan, full `config.h`, etc).

Configurations

We provide some non-standard configurations focused on specific use cases in the `configs/` directory. You can read more about those in `configs/README.txt`

Porting mbed TLS
---

mbed TLS can be ported to many different architectures, OS's and platforms. Before starting a port, you may find the following knowledge base articles useful:

- [Porting mbed TLS to a new environment or OS](https://tls.mbed.org/kb/how-to/how-do-i-port-mbed-tls-to-a-new-environment-OS)
- [What external dependencies does mbed TLS rely on?](https://tls.mbed.org/kb/development/what-external-dependencies-does-mbedtls-rely-on)
- [How do I configure mbed TLS](https://tls.mbed.org/kb/compiling-and-building/how-do-i-configure-mbedtls)

Contributing

We gratefully accept bug reports and contributions from the community. There are some requirements
 we need to fulfill in order to be able to integrate contributions:

- All contributions, whether large or small require a Contributor's License Agreement (CLA) to be accepted. This is because source code can possibly fall under copyright law and we need your consent to share in the ownership of the copyright.
- We would ask that contributions conform to [our coding standards](https://tls.mbed.org/kb/development/mbedtls-coding-standards), and that contributions should be fully tested before submission.
- As with any open source project, contributions will be reviewed by the project team and community and may need some modifications to be accepted.

To accept the Contributors Licence Agreement (CLA), individual contributors can do this by creating an mbed account and [accepting the online agreement here with a click through](https://developer.mbed.org/contributor_agreement/). Alternatively, for contributions from corporations, or those that do not wish to create an mbed account,

a slightly different agreement can be found [here](https://www.mbed.com/en/about-mbed/contributor-license-agreements/). This agreement should be signed and returned to ARM as described in the instructions given.

Making a Contribution

1. [Check for open issues](https://github.com/ARMmbed/mbedtls/issues) or [start a discussion](https://tls.mbed.org/discussions) around a feature idea or a bug.
2. Fork the [mbed TLS repository on GitHub](https://github.com/ARMmbed/mbedtls) to start making your changes. As a general rule, you should use the "development" branch as a basis.
3. Write a test which shows that the bug was fixed or that the feature works as expected.
4. Send a pull request and bug us until it gets merged and published. Contributions may need some modifications, so work with us to get your change accepted. We will include your name in the ChangeLog :)

-----BEGIN CERTIFICATE-----
MIIDwjCCAaqgAwIBAgIBEDANBgkqhkiG9w0BAQsFADBIMQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxJjAkBgNVBAMTHVBvbGFyU1NMIFRlc3QgSW50ZXJt
ZWRpYXRlIENBMB4XDTEzMDkyNDE2MTIyNFoXDTIzMDkyMjE2MTIyNFowNDELMAk G
A1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NMMRIwEAYDVQQDEwlsb2NhbGhvc3Qw
WTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQcbffp2qXqoZyychmoCRxzrd4Vu96m
47NPBehtEC46aTeXgDnBdf++znABrAtfXBRNQz8ARIeYBmskr22rlKjyo4GVMIGS
MAkGA1UdEwQCMAAwHQYDVR0OBBYEFNIK06V3H85VsFxGoo5zbL+hYCa7MGYGA1Ud
IwRfMF2AFDh32Gt3nCh3gotO2BupHveUFrcOoUKkQDA+MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0GC
AQ4wDQYJKoZIhvcNAQELBQADggIBADRoQ5fHKw+vkl0D3aqLX1XrZidb+25AWbhr
FYXdaskN219PrXBL3cV8x5tK6qsPKSyyw1lue80OmhXs/w7PJkOHHUSWRnmTv7lr
8Us3Zr/yOF/VVqzdGs7DlOTpyzEBdugI9uar/aCqHDoltN8wOduOoQB9aojYpROj
+gjlEO0mgt/87XpjYOig1o0jv44QYDQZQzpj1zeIn6WMe6xk9YDwCLMjRIpg++c7
QyxvcEJTn80wX1SaEBM2gau97G7bORLMwBVkMT4oSY+iKYgpPpawOnMJbqUP73Dm
yfJExDdrW/BbWZ/vKIcSqSZIbkHdkNjUDVHczyVwQxZxzvLFw/B1k9s7jYFsi5eK
TNAdXFa4et1H2sd+uhu24GxsjmJioDrftixcgzPVBjDCjH8QWkBEX292WJ58on0e
deWLpZUnzPdE1B4rsiPw1Vg28mGgr2O1xgBQr/fx6A+8ItNTzAXbZfEcult9ypwM
0b6YDNe5IvdKk8iwz3mof0VNy47K6xoCaE/fxxWkjoXK8x2wfswGeP2QgUzQE93b
OtjdHpsG1c7gIVFQmKATyAPUz4vqmezgNRleXU0oL0PYtoCmKQ51UjNMUfmO9xCj
VJaNa2iTQ5Dgic+CW4TYAgj5/9g9X3WfwnDNxrZ0UxxawGElczHXqbrNleTtPaKp
a8Si6UK5
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEATCCA4egAwIBAgIBDjAKBggqhkjOPQQDAjA+MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EwHhcN
MTMwOTI0MTU1NTE0WhcNMjMwOTIyMTU1NTE0WjBIMQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxJjAkBgNVBAMTHVBvbGFyU1NMIFRlc3QgSW50ZXJtZWRp
YXRlIENBMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAo1Oc8nr6fMTq
vowV+CpC55i5BZGFGc50Eb4RLBSRTH1e7JepdFjAVbBtyQRJSiY1ja0tgLQDDKZR
wfEI+b4azse460InPHv7C1TN0upXlxuj6m9B1IlP+sBaM7WBC6dVfPO+jVMIxgkF
CaBCLhhdK1Fjf8HjkT/PkctWnho8NTwivc9+nqRZjXe/eIcqm5HwjDDhu+gz+o0g
Vz9MfZNi1JyCrOyNZcy+cr2QeNnNVGnFq8xTxtu6dLunhpmLFj2mm0Vjwa7Ypj5q
AjpqTMtDvqbRuToyoyzajhMNcCAf7gwzIupJJFVdjdtgYAcQwzikwF5HoITJzzJ2
qgxF7CmvGZNb7G99mLdLdhtclH3wAQKHYwEGJo7XKyNEuHPQgB+e0cg1SD1HqlAM

uCfGGTWQ6me7Bjan3t0NzoTdDq6IpKTesbaY+/9e2xn8DCrhBKLXQMZFDZqUoLYA
kGPOEGgvlPnIIXAawouxCaNYEh5Uw871YMSPT28rLdFr49dwYOtDg9foA8hDIW2P
d6KXbrZteesvA1nYzEOs+3AjrbT79Md2W8Bz9bqBVNlNOESSqm4kiCJFmslm/6br
Np0MSQd+o22PQ4xRtmP6UsTfU0ueiMpYc8TYYhMbfnfFyo4m707ebcflPbBEN2dg
updQ66cvfCJB0QJt9upafY0lpdV1qUkCAwEAAaOBoDCBnTAdBgNVHQ4EFgQUOHfY
a3ecKHeCi07YG6ke95QWtw4wbgYDVR0jBGcwZYAUnW0gJEkBPyvLeLUZvH4kydv7
NnyhQqRAMD4xCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UE
AxMTUG9sYXJzc2wgVGVzdCBFQyBDQYIJAMFD4n5iQ8zoMAwGA1UdEwQFMAMBAf8w
CgYIKoZIzj0EAwIDaAAwZQIxAPyE+u+eP7gRrSFjQicmpYg8jiFUCYEowWY2zuOG
i1HXYwmpDHfasQ3rNSuf/gHvjwIwbSSjumDk+uYNci/KMELDsD0MFHxZhhBc9Hp9
Af5cNR8KhzegznL6amRObGGKmX1F
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIC+jCCAeKgAwIBAgIBATANBgkqhkiG9w0BAQsFADAWMRQwEgYDVQQDEwtUZXN0
IHJvb3QgMjAeFw0wMTAxMDEwMDAwMDBaFw0zMDEyMzEyMzU5NTlaMBYxFDASBgNV
BAMTC1Rlc3Qgcm9vdCAyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
mTX2sHY42Ord9gWyB6GcdlLjjE+4zBJ1BoDpMnvJ89niMTuZTq1ViMp/B6RuTH+2
YF3+riZYQDH9yM/8rgvAUIvK9STaq19Zrm0mnfQUo9yKdkfoJ+XvWuvK6f+NkAMg
xfhAD6eSupigTvov/w2IT8rS0dxo4KF6hKBL2aYlXhiEyi/NmsEPZWvVh+qk3L/Q
GSwpgC+DhVoQzFRofUdK9O9MkgR675iftaFDvyi7F0fxrSLfB/Wy4cgRYzIW6pyN
2sXWivKdLI3bgB01ffdbO17ZAGILK1whO29/bX6hbH09Y/H7jR2vjy+KP9N0PEa3
7SBymlokB3A8wq/LWPYPeQIDAQABo1MwUTAPBgNVHRMECDAGAQEBAgEAMB0GA1Ud
DgQWBBSOBd1fH00Y9r5S8cELj/9IT4BGlDAfBgNVHSMEGDAWgBSOBd1fH00Y9r5S
8cELj/9IT4BGlDANBgkqhkiG9w0BAQsFAAOCAQEAFEY2StppaPzOgG6vEvPJr//+
NWY1jKcBB3cT+zWJW54+BexDjyaBRnBIPvRLDG8PAlhlYr9v/P6JCjBSuhYorFLG
P4ZhD+akuMvn6yF7nsyG20LHPwvE7/jye7+zSO3hhyqCg7N7M7O17exo/agw/iUI
DYUuUv1ZJlZvPB2kmZMYa78g0P2ynyKpu4hdbstJzxwA4aQDXGQxcQNtv+3ZCdC2
TI4w0jodkjqdq/4y0McpkEvYL3/LaQElLaHr8CQo7xYEzsjv+cnzojCO/ilXU+Rl
sz940Q4njAJqlpfiJ44aFytjp96uN4YVpViFCvRz//9uyQY9kuA/8kKwJuO3qw==
-----END
CERTIFICATE-----
-----BEGIN X509 CRL-----
MIIBbzCB9gIBATAJBgcqhkjOPQQBMD4xCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQ
b2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBFQyBDQRcNMTMwOTI0MTYz
MTA4WhcNMjMwOTIyMTYzMTA4WjAUMBICAQoXDTEzMDkyNDE2MjgzOFqgcjBwMG4G
A1UdIwRnMGWAFJ1tICRJAT8ry3i1Gbx+JMnb+zZ8oUKkQDA+MQswCQYDVQQGEwJO
TDERMA8GA1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMg
Q0GCCQDBQ+J+YkPM6DAJBgcqhkjOPQQBA2kAMGYCMQDVG95rrSSl4dJgbJ5vR1GW
svEuEsAh35EhF1WrcadMuCeMQVX9cUPupFfQUpHyMfoCMQCKf0yv8pN9BAoi3FVm
56meWPhUekgLKKMAobt2oJJY6feuiFU2YFGs1aF0rV6Bj+U=
-----END X509 CRL-----
-----BEGIN X509 CRL-----
MIIBcTCB9wIBATAKBggqhkjOPQQDBDA+MQswCQYDVQQGEwJOTDERMA8GA1UEChMI
UG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EXDTEzMDkyNDE2
MzEwOFoXDTIzMDkyMjE2MzEwOFowFDASAgEKFw0xMzA5MjQxNjI4MzhaoHIwcDBu
BgNVHSMEZzBlgBSdbSAkSQE/K8t4tRm8fiTJ2/s2fKFCpEAwPjELMAkGA1UEBhMC
TkwxETAPBgNVBAoTCFBvbGFyU1NMMRwwGgYDVQQDExNQb2xhcnNzbCBUZXN0IEVD

IENBggkAwUPifmJDzOgwCgYIKoZIzj0EAwQDaQAwZgIxAL/VFrDIYUECsS0rVpAy
6zt/CqeAZ1sa/l5LTaG1XW286n2Kibipr6EpkYZNYIQILgIxAI0wb3Py1DHPWpYf
/BFBH7C3KYq+nWTrLeEnhrjU1LzG/CiQ8lnuskya6lw/P3lJ/A==
-----END
X509 CRL-----
-----BEGIN CERTIFICATE-----
MIIDWzCCAhKgAwIBAgIBGDA+BgkqhkiG9w0BAQowMaANMAsGCWCGSAFlAwQCAaEa
MBgGCSqGSIb3DQEBCDALBglghkgBZQMEAgGiBAICAN4wOzELMAkGA1UEBhMCTkwx
ETAPBgNVBAoTCFBvbGFyU1NMMRkwFwYDVQQDExBQb2xhclNTTCBUZXN0IENBMB4X
DTE0MDEyMDEzNTc0NVoXDTI0MDExODEzNTc0NVowNDELMAkGA1UEBhMCTkwxETAP
BgNVBAoTCFBvbGFyU1NMMRIwEAYDVQQDEwlsb2NhbGhvc3QwgZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBAN0Rip+ZurBoyirqO2ptWZftTslU5A3uzqB9oB6q6A7C
uxNA24oSjokTJKXF9frY9ZDXyMrLxf6THa/aEiNzUnlGGrqgVyt2FjGzqK/nOJsI
i2OZOgol7kXSGFi6uZMa7dRYmmMbN/z3FAifhWVJ81kybdHg6G3eUu1mtKkL2kCV
AgMBAAGjgZIwgY8wCQYDVR0TBAIwADAdBgNVHQ4EFgQU7vPH9R8VpU1HicHTImOy
36fOvVEwYwYDVR0jBFwwWoAUtFrkpbPe0lL2udWmlQ/rPrzH/f+hP6Q9MDsxCzAJ
BgNVBAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEZMBcGA1UEAxMQUG9sYXJTU0wg
VGVzdCBDQYIBADA+BgkqhkiG9w0BAQowMaANMAsGCWCGSAFlAwQCAaEaMBgGCSqG
SIb3DQEBCDALBglghkgBZQMEAgGiBAICAN4DggEBAH0+knqkcLaxeDkenBQgd4Qg
3ZyAhtpiLU689mw+3cXB/uzFrCIxEL5aGh1eSj+DszB+FtsZ06ux7JVQqVOA2Wm9
yLxC6wF8OOYj0nBa91BWLhRAHLhmIdWsVk7Hl9KojZd4TwV2N+ZEV/BLxyoRvK4H
V4xCpzgDSiTPe8Etk4r+0akbr6bsOUBayPb7MGLHubZKq8NsFAmmynp+fPmHd3SE
0ooJdiZ1MmKPKLE5Og/hXCI8qeiXQUR6oQ7b2XONsrI2HIj2SA9dA5qmHwE5PbMu
zqxQ3R83boqLXbkFORn+UiYLmffqdoWuNy00BHMCrxRA9DUv+WyN4npLMF8rOJw=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDhDCCAmygAwIBAgIBHzANBgkqhkiG9w0BAQsFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTQwMzI2MDkyMzEyWhcNMjQwMzIzMDkyMzEyWjA7MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEHBvbGFyc3NsLmV4YW1wbGUwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCpAh89QGrVVVOL/TbugmUuFWFeib+4
6EWQ2+6IFlLT8UNQR5YSWWSHa/0r4Eb5c77dz5LhkVvtZqBviSl5RYDQg2rVQUN3
Xzl8CQRHgrBXOXDto+wVGR6oMwhHwQVCqf1Mw7Tf3QYfTRBRQGdzEw9A+G2BJV8K
sVPGMH4VOaz5Wu5/kp6mBVvnE5eFtSOS2dQkBtUJJYl1B92mGo8/CRm+rWUsZOuV
m9z+QV4XptpsW2nMAroULBYknErczdD3Umdz8S2gI/1+9DHKLXDKiQsE2y6mT3Bu
ns69WIniU1meblqSZeKIPwyUGaPd5eidlRPtKdurcBLcWsprF6tSglSxAgMBAAGj
gZIwgY8wCQYDVR0TBAIwADAdBgNVHQ4EFgQUH3TWPynBdHRFOwUSLD2ovUNZAqYw
YwYDVR0jBFwwWoAUtFrkpbPe0lL2udWmlQ/rPrzH/f+hP6Q9MDsxCzAJBgNVBAYT
Ak5MMREwDwYDVQQKEwhQb2xhclNTTDEZMBcGA1UEAxMQUG9sYXJTU0wgVGVzdCBD
QYIBADANBgkqhkiG9w0BAQsFAAOCAQEAXs4vQqlIlxrMbE6IwAHLcGJuz17Ru/en
H9bUnnSh1pxa+NHMKZHBG3GT0iaxsVtXf56/tXH4+HL7ntJjrczGN1PbhMGPyt94
556ZgDxkHT9k7KjPAIs9BrjFHvl9NyIZzcbwkiC0qGvdzjSfe3AiSYuhXI/9/Hog
uUwReH+T2U/ICEHQ5O8aV5nvpgqL3EeEmyx3bu+YXtZMWQUYzX+ya4TnKVPdqwbf
ebr6v1hLXrUFl6rZ3wEJ6MqUW3SGZRkCVNZUOD6Ky3+EiLwYFhuKGdFqSS0JAAD7
ZO3yPu5hu3BhAQYavK4Yyfi9IQmubBqxopPwyzjG1HPw2lj+oapH0w==
-----END

CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIBzDCCAVOgAwIBAgIJAP6mZLzh0IPSMAoGCCqGSM49BAMCMD4xCzAJBgNVBAYT
Ak5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBF
QyBDQTAeFw0xNDA0MDkxMTIzMzhaFw0yNDA0MDYxMTIzMzhaMD4xCzAJBgNVBAYT
Ak5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBF
QyBDQTB2MBAGByqGSM49AgEGBSuBBAAiA2IABMPaKzRBN1gvh1b+/Im6KUNLTuBu
ww5XUzM5WNRStJGVOQsj318XJGJI/BqVKc4sLYfCiFKAr9ZqqyHduNMcbli4yuiy
aY7zQa0pw7RfdadHb9UZKVVpmlM7ILRmFmAzHqMdMBswDAYDVR0TBAUwAwEB/zAL
BgNVHQ8EBAMCAQIwCgYIKoZIzj0EAwIDZwAwZAIwZOCKY0EHXYzI4cQsFnfOrxm1
ufvNeZ4ZcSZWrkTBazW2OBCuCP9SLznec3SFOUvvAjAKe/qycfxkHivjieCEG1Kt
m2D4QKSJELUhTHr4zdkeqbzgui0y3iouaoyWsKvetNg=
-----END CERTIFICATE-----
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
   <Configuration>Release</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\pkey\rsa_sign.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">

  <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid>{10790F49-6887-AAB6-2D86-BCBD516F8D26}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>rsa_sign</RootNamespace>
 </PropertyGroup>

```
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
   <UseDebugLibraries>true</UseDebugLibraries>
   <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
   <UseDebugLibraries>true</UseDebugLibraries>
   <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
    <ConfigurationType>Application</ConfigurationType>
   <UseDebugLibraries>false</UseDebugLibraries>
   <WholeProgramOptimization>true</WholeProgramOptimization>
   <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
   <UseDebugLibraries>false</UseDebugLibraries>
   <WholeProgramOptimization>true</WholeProgramOptimization>
   <CharacterSet>Unicode</CharacterSet>
   <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
 />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
    <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
```

```
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
     <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
 <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
```

<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
<AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
</Link>
<ProjectReference>
<LinkLibraryDependencies>false</LinkLibraryDependencies>
</ProjectReference>
</ItemDefinitionGroup>
<ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
<ClCompile>
<WarningLevel>Level3</WarningLevel>
<PrecompiledHeader>
</PrecompiledHeader>
<Optimization>MaxSpeed</Optimization>
<FunctionLevelLinking>true</FunctionLevelLinking>
<IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
<AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
</ClCompile>
<Link>
<SubSystem>Console</SubSystem>
<GenerateDebugInformation>true</GenerateDebugInformation>
<EnableCOMDATFolding>true</EnableCOMDATFolding>
<OptimizeReferences>true</OptimizeReferences>
<AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
</Link>
</ItemDefinitionGroup>
<ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
<ClCompile>
<WarningLevel>Level3</WarningLevel>
<PrecompiledHeader>
</PrecompiledHeader>
<Optimization>MaxSpeed</Optimization>
<FunctionLevelLinking>true</FunctionLevelLinking>
<IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
<AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
</ClCompile>
<Link>
<SubSystem>Console</SubSystem>
<GenerateDebugInformation>true</GenerateDebugInformation>
<EnableCOMDATFolding>true</EnableCOMDATFolding>
<OptimizeReferences>true</OptimizeReferences>
<AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>

```
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
 <Import
 Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
    <Configuration>Debug</Configuration>
    <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
    <Configuration>Debug</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
    <Configuration>Release</Configuration>
    <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
    <Configuration>Release</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\random\gen_random_ctr_drbg.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">
    <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid>{5FCC71F6-FF33-EBCF-FBA2-8FC783D5318E}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>gen_random_ctr_drbg</RootNamespace>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
```

```
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
   <UseDebugLibraries>true</UseDebugLibraries>
   <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'"
 Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
   <UseDebugLibraries>false</UseDebugLibraries>
   <WholeProgramOptimization>true</WholeProgramOptimization>
   <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
   <UseDebugLibraries>false</UseDebugLibraries>
   <WholeProgramOptimization>true</WholeProgramOptimization>
   <CharacterSet>Unicode</CharacterSet>
   <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')"
 Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup
 Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
   <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
```

```
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
```

```
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
     <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
  </Link>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
```

```
  <Import Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
```

```
-----BEGIN CERTIFICATE-----
MIIB4zCCAWmgAwIBAgIBOjAKBggqhkjOPQQDAjA+MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EwHhcN
MTQwNDEwMTcyMDQxWhcNMjQwNDA3MTcyMDQxWjA0MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxEjAQBgNVBAMTCWxvY2FsaG9zdDBZMBMGByqGSM49AgEG
CCqGSM49AwEHA0IABDfMVtl2CR5acj7HWS3/IG7ufPkGkXTQrRS192giWWKSTuUA
2CMR/+ov0jRdXRa9iojCa3cNVc2KKg76Aci07f+jYjBgMAkGA1UdEwQCMAAwHQYD
VR0OBBYEFFBhpY/UB9nXggEM5WV/jGNGpxO+MB8GA1UdIwQYMBaAFJ1tICRJAT8r
y3i1Gbx+JMnb+zZ8MBMGA1UdJQQMMAoGCCsGAQUFBwMDMAoGCCqGSM49BAMCA2gA
MGUCMQC294oVK6fUjH/abI1xzytTusi8dl7518L0Y19q8zi9K19OtxzPK09h7xyy
gaJRvpUCMFS6hYhrht38yqwwhSVlnmTMVtira58mEUhL6v7Qzw1sz/Dm4aXkW3s6
JQV1kqqbRw==
-----END CERTIFICATE-----
-----BEGIN PUBLIC KEY-----
MEkwEwYHKoZIzj0CAQYIKoZIzj0DAQEDMgAEvHl9s65/COw9SWtPtBGz9iClWKUB
4CItCM/g3Irsixp78kvpKVHMW6G+uyR0kJrg
-----END PUBLIC KEY-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTMwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTQwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATRMZN0RHzP
donNmZuq9XPhzvQ52TaokxT39qpQtlFyvUuEGKrLoNvdcpARaA0rGput6RLAQOVU
iNVlJ3Ipj789o4GJMIGGMB0GA1UdDgQWBBRNsJB++ccSBmbCCKBxi4CjXROBkzBX
BgNVHSMEUDBOgBTmVnUSF2MYwws/nCMv7b1wJVkDmqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTEyggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgVfuLpjp08AaxKWf6cuZUUCRd7CojSS1I
71hzeUyFS+sCIQDNJI6P/pBbiHgTaGlBAgfcEfmxmbY0n4xZndtxIkmyVA==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB+zCCAYCgAwIBAgIBATAMBggqhkjOPQQDAgUAMD4xCzAJBgNVBAYTAk5MMREw
DwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBFQyBDQTAe
Fw0yMzA5MjIxNTQ5NDlaFw0zMDEyMzEyMzEyMzU5NTlaMD4xCzAJBgNVBAYTAk5MMREw
DwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBFQyBDQTB2
MBAGByqGSM49AgEGBSuBBAAiA2IABMPaKzRBN1gvh1b+/Im6KUNLTuBuww5XUzM5
WNRStJGVOQsj318XJGJI/BqVKc4sLYfCiFKAr9ZqqyHduNMcbli4yuiyaY7zQa0p
w7RfdadHb9UZKVVpmlM7ILRmFmAzHqNQME4wDAYDVR0TBAUwAwEB/zAdBgNVHQ4E
FgQUnW0gJEkBPyvLeLUZvH4kydv7NnwwHwYDVR0jBBgwFoAUnW0gJEkBPyvLeLUZ
vH4kydv7NnwwDAYIKoZIzj0EAwIFAANnADBkAjB1ZNdOM7KRJiPo45hP17A1sJSH
qHFPEJbml6KdNevoVZ1HqvP8AoFGcPJRpQVtzC0CMDa7JEqn0dOss8EmW9pVF/N2
+XvzNczj89mWMgPhJJlT+MONQx3LFQO+TMSI9hLdkw==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIICUjCCAdegAwIBAgIJAMFD4n5iQ8zoMAoGCCqGSM49BAMCMD4xCzAJBgNVBAYT
```

Ak5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBF
QyBDQTAeFw0xMzA5MjQxNTQ5NDhaFw0yMzA5MjIxNTQ5NDhaMD4xCzAJBgNVBAYT
Ak5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBF
QyBDQTB2MBAGByqGSM49AgEGBSuBBAAiA2IABMPaKzRBN1gvh1b+/Im6KUNLTuBu
ww5XUzM5WNRStJGVOQsj318XJGJI/BqVKc4sLYfCiFKAr9ZqqyHduNMcbli4yuiy
aY7zQa0pw7RfdadHb9UZKVVpmlM7ILRmFmAzHqOBoDCBnTAdBgNVHQ4EFgQUnW0g
JEkBPyvLeLUZvH4kydv7NnwwbgYDVR0jBGcwZYAUnW0gJEkBPyvLeLUZvH4kydv7
NnyhQqRAMD4xCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UE
AxMTUG9sYXJzc2wgVGVzdCBFQyBDQYIJAMFD4n5iQ8zoMAwGA1UdEwQFMAMBAf8w
CgYIKoZIzj0EAwIDaQAwZgIxAMO0YnNWKJUAfXgSJtJxexn4ipg+kv4znuR50v56
t4d0PCu412mUC6Nnd7izvtE2MgIxAP1nnJQjZ8BWukszFQDG48wxCCyci9qpdSMv
uCjn8pwUOkABXK8Mss90fzCfCEOtIA==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEATCCA4egAwIBAgIBDjAKBggqhkjOPQQDAjA+MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EwHhcN
MTMwOTI0MTU1NTE0WhcNMjMwOTIyMTU1NTE0WjBIMQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxJjAkBgNVBAMTHVBvbGFyU1NMIFRlc3QgSW50ZXJtZWRp
YXRlIENBMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAo1Oc8nr6fMTq
vowV+CpC55i5BZGFGc50Eb4RLBSRTH1e7JepdFjAVbBtyQRJSiY1ja0tgLQDDKZR
wfEI+b4azse460InPHv7C1TN0upXlxuj6m9B1IlP+sBaM7WBC6dVfPO+jVMIxgkF
CaBCLhhdK1Fjf8HjkT/PkctWnho8NTwivc9+nqRZjXe/eIcqm5HwjDDhu+gz+o0g
Vz9MfZNi1JyCrOyNZcy+cr2QeNnNVGnFq8xTxtu6dLunhpmLFj2mm0Vjwa7Ypj5q
AjpqTMtDvqbRuToyoyzajhMNcCAf7gwzIupJJFVdjdtgYAcQwzikwF5HoITJzzJ2
qgxF7CmvGZNb7G99mLdLdhtclH3wAQKHYwEGJo7XKyNEuHPQgB+e0cg1SD1HqlAM
uCfGGTWQ6me7Bjan3t0NzoTdDq6IpKTesbaY+/9e2xn8DCrhBKLXQMZFDZqUoLYA
kGPOEGgvlPnIIXAawouxCaNYEh5Uw871YMSPT28rLdFr49dwYOtDg9foA8hDIW2P
d6KXbrZteesvA1nYzEOs+3AjrbT79Md2W8Bz9bqBVNlNOESSqm4kiCJFmslm/6br
Np0MSQd+o22PQ4xRtmP6UsTfU0ueiMpYc8TYYhMbfnfFyo4m707ebcflPbBEN2dg
updQ66cvfCJB0QJt9upafY0lpdV1qUkCAwEAAaOBoDCBnTAdBgNVHQ4EFgQUOHfY
a3ecKHeCi07YG6ke95QWtw4wbgYDVR0jBGcwZYAUnW0gJEkBPyvLeLUZvH4kydv7
NnyhQqRAMD4xCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UE
AxMTUG9sYXJzc2wgVGVzdCBFQyBDQYIJAMFD4n5iQ8zoMAwGA1UdEwQFMAMBAf8w
CgYIKoZIzj0EAwIDaAAwZQIxAPyE+u+eP7gRrSFjQicmpYg8jiFUCYEowWY2zuOG
i1HXYwmpDHfasQ3rNSuf/gHvjwIwbSSjumDk+uYNci/KMELDsD0MFHxZhhBc9Hp9
Af5cNR8KhzegznL6amRObGGKmX1F
-----END
CERTIFICATE-----
-----BEGIN EC PARAMETERS-----
BggqhkjOPQMBBw==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIM0YCnGkEG/TjBxrytP9Ztslm1yoQaWptBxegRzzBRDVoAoGCCqGSM49
AwEHoUQDQgAEO1bKeyZgzZID4f/s5iD5He6NMaLf1jzBZ97gLBrbFN/OTBdH5oXx
S4UW2x/YeCY2B4/MtLKVN27lF4X7bwGVWw==
-----END EC PRIVATE KEY-----

-----BEGIN X509 CRL-----
MIICejCCATECAQEwPgYJKoZIhvcNAQEKMDGgDTALBglghkgBZQMEAgKhGjAYBgkq
hkiG9w0BAQgwCwYJYIZIAWUDBAICogQCAgDOMDsxCzAJBgNVBAYTAk5MMREwDwYD
VQQKEwhQb2xhclNTTDEZMBcGA1UEAxMQUG9sYXJTU0wgVGVzdCBDQRcNMTQwMTIw
MTM1NjI4WhcNMjQwMTE4MTM1NjI4WjAoMBICAQoXDTEzMDkyNDE2MjgzOFowEgIB
FhcNMTQwMTIwMTM0MzA1WqBnMGUwYwYDVR0jBFwwWoAUtFrkpbPe0lL2udWmlQ/r
PrzH/f+hP6Q9MDsxCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEZMBcG
A1UEAxMQUG9sYXJTU0wgVGVzdCBDQYIBADA+BgkqhkiG9w0BAQowMaANMAsGCWCG
SAFlAwQCAqEaMBgGCSqGSIb3DQEBCDALBglghkgBZQMEAgKiBAICAM4DggEBAAco
SntUGDLBOAu0IIZaVea5Nt1NMsMcppC0hWPuH1LKAwyUODBqpT+0+AuALK0eIdYR
a7mAB+cv2fFwmwxnQWJ1Fvx4ft/N2AAfB83VRKpSo3xR8bxloHfTWKmyxJHmH9j1
EYmLS86rj3Nhjf4m/YlQQ3Im5HwOgSgBOE8glq5D+0Wmsi9LsNEZXEzMw7TMUgbs
y9o/ghYF/shKU4mewK3DeM9gQiTcH5A4ISXR87hBQ08AKJRAG1CLvTyzqWiUUY+k
q8iZDYF17sHrPi2yn8q9c4zdxiaWDGDdL0Lh90wXGTAageoGEq25TMuL5FpX+u1u
KUH/xf1jEnNzbYNGiZw=
-----END X509 CRL-----
-----BEGIN CERTIFICATE-----
MIICUjCCAdegAwIBAgIJAMFD4n5iQ8zoMAoGCCqGSM49BAMCMD4xCzAJBgNVBAYT
Ak5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBF
QyBDQTAeFw0xMzA5MjQxNTQ5NDhaFw0yMzA5MjIxNTQ5NDhaMD4xCzAJBgNVBAYT
Ak5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBF
QyBDQTB2MBAGByqGSM49AgEGBSuBBAAiA2IABMPaKzRBN1gvh1b+/Im6KUNLTuBu
ww5XUzM5WNRStJGVOQsj318XJGJI/BqVKc4sLYfCiFKAr9ZqqyHduNMcbli4yuiy
aY7zQa0pw7RfdadHb9UZKVVpmlM7ILRmFmAzHqOBoDCBnTAdBgNVHQ4EFgQUnW0g
JEkBPyvLeLUZvH4kydv7NnwwbgYDVR0jBGcwZYAUnW0gJEkBPyvLeLUZvH4kydv7
NnyhQqRAMD4xCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UE
AxMTUG9sYXJzc2wgVGVzdCBFQyBDQYIJAMFD4n5iQ8zoMAwGA1UdEwQFMAMBAf8w
CgYIKoZIzj0EAwIDaQAwZgIxAMO0YnNWKJUAfXgSJtJxexn4ipg+kv4znuR50v56
t4d0PCu412mUC6Nnd7izvtE2MgIxAP1nnJQjZ8BWukszFQDG48wxCCyci9qpdSMv
uCjn8pwUOkABXK8Mss90fzCfCEOtIA==
-----END CERTIFICATE-----
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 0 (0x0)
    Signature Algorithm: sha1WithRSAEncryption

   Issuer: C=NL, O=PolarSSL, CN=PolarSSL Test CA
    Validity
      Not Before: Feb 12 14:44:00 2011 GMT
      Not After : Feb 12 14:44:00 2021 GMT
    Subject: C=NL, O=PolarSSL, CN=PolarSSL Test CA
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (2048 bit)
        Modulus (2048 bit):
          00:c0:df:37:fc:17:bb:e0:96:9d:3f:86:de:96:32:
          7d:44:a5:16:a0:cd:21:f1:99:d4:ec:ea:cb:7c:18:

58:08:94:a5:ec:9b:c5:8b:df:1a:1e:99:38:99:87:
1e:7b:c0:8d:39:df:38:5d:70:78:07:d3:9e:d9:93:
e8:b9:72:51:c5:ce:a3:30:52:a9:f2:e7:40:70:14:
cb:44:a2:72:0b:c2:e5:40:f9:3e:e5:a6:0e:b3:f9:
ec:4a:63:c0:b8:29:00:74:9c:57:3b:a8:a5:04:90:
71:f1:bd:83:d9:3f:d6:a5:e2:3c:2a:8f:ef:27:60:
c3:c6:9f:cb:ba:ec:60:7d:b7:e6:84:32:be:4f:fb:
58:26:22:03:5b:d4:b4:d5:fb:f5:e3:96:2e:70:c0:
e4:2e:bd:fc:2e:ee:e2:41:55:c0:34:2e:7d:24:72:
69:cb:47:b1:14:40:83:7d:67:f4:86:f6:31:ab:f1:
79:a4:b2:b5:2e:12:f9:84:17:f0:62:6f:27:3e:13:
58:b1:54:0d:21:9a:73:37:a1:30:cf:6f:92:dc:f6:
e9:fc:ac:db:2e:28:d1:7e:02:4b:23:a0:15:f2:38:
65:64:09:ea:0c:6e:8e:1b:17:a0:71:c8:b3:9b:c9:
ab:e9:c3:f2:cf:87:96:8f:80:02:32:9e:99:58:6f:
a2:d5
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints:
CA:TRUE
X509v3 Subject Key Identifier:
B4:5A:E4:A5:B3:DE:D2:52:F6:B9:D5:A6:95:0F:EB:3E:BC:C7:FD:FF
X509v3 Authority Key Identifier:
keyid:B4:5A:E4:A5:B3:DE:D2:52:F6:B9:D5:A6:95:0F:EB:3E:BC:C7:FD:FF
DirName:/C=NL/O=PolarSSL/CN=PolarSSL Test CA
serial:00

Signature
Algorithm: sha1WithRSAEncryption
b8:fd:54:d8:00:54:90:8b:25:b0:27:dd:95:cd:a2:f7:84:07:
1d:87:89:4a:c4:78:11:d8:07:b5:d7:22:50:8e:48:eb:62:7a:
32:89:be:63:47:53:ff:b6:be:f1:2e:8c:54:c0:99:3f:a0:b9:
37:23:72:5f:0d:46:59:8f:d8:47:cd:97:4c:9f:07:0c:12:62:
09:3a:24:e4:36:d9:e9:2c:da:38:d0:73:75:61:d7:c1:6c:26:
8b:9b:e0:d5:dc:67:ed:8c:6b:33:d7:74:22:3c:4c:db:b5:8d:
2a:ce:2c:0d:08:59:05:09:05:a6:39:9f:b3:67:1b:e2:83:e5:
e1:8f:53:f6:67:93:c7:f9:6f:76:44:58:12:e8:3a:d4:97:e7:
e9:c0:3e:a8:7a:72:3d:87:53:1f:e5:2c:84:84:e7:9a:9e:7f:
66:d9:1f:9b:f5:13:48:b0:4d:14:d1:de:b2:24:d9:78:7d:f5:
35:cc:58:19:d1:d2:99:ef:4d:73:f8:1f:89:d4:5a:d0:52:ce:
09:f5:b1:46:51:6a:00:8e:3b:cc:6f:63:01:00:99:ed:9d:a6:
08:60:cd:32:18:d0:73:e0:58:71:d9:e5:d2:53:d7:8d:d0:ca:
e9:5d:2a:0a:0d:5d:55:ec:21:50:17:16:e6:06:4a:cd:5e:de:
f7:e0:e9:54
-----BEGIN CERTIFICATE-----
MIIDhzCCAm+gAwIBAgIBADANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTEwMjEyMTQ0NDAwWhcNMjEwMjEyMTQ0NDAwWjA7MQswCQYDVQQGEwJOTDERMA8G

A1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDA3zf8F7vglp0/ht6WMn1EpRagzSHx
mdTs6st8GFgIlKXsm8WL3xoemTiZhx57wI053zhdcHgH057Zk+i5clHFzqMwUqny
50BwFMtEonILwuVA+T7lpg6z+exKY8C4KQB0nFc7qKUEkHHxvYPZP9al4jwqj+8n
YMPGn8u67GB9t+aEMr5P+1gmIgNb1LTV+/Xjli5wwOQuvfwu7uJBVcA0Ln0kcmnL
R7EUQIN9Z/SG9jGr8XmksrUuEvmEF/Bibyc+E1ixVA0hmnM3oTDPb5Lc9un8rNsu
KNF+AksjoBXyOGVkCeoMbo4bF6BxyLObyavpw/LPh5aPgAIynplYb6LVAgMBAAGj
gZUwgZIwDAYDVR0TBAUwAwEB/zAdBgNVHQ4EFgQUtFrkpbPe0lL2udWmlQ/rPrzH
/f8wYwYDVR0jBFwwWoAUtFrkpbPe0lL2udWmlQ/rPrzH/f+hP6Q9MDsxCzAJBgNV
BAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEZMBcGA1UEAxMQUG9sYXJTU0wgVGVz
dCBDQYIBADANBgkqhkiG9w0BAQUFAAOCAQEAuP1U2ABUkIslsCfdlc2i94QHHYeJ
SsR4EdgHtdciUI5I62J6Mom+Y0dT/7a+8S6MVMCZP6C5NyNyXw1GWY/YR82XTJ8H
DBJiCTok5DbZ6SzaONBzdWHXwWwmi5vg1dxn7YxrM9d0IjxM27WNKs4sDQhZBQkF
pjmfs2cb4oPl4Y9T9meTx/lvdkRYEug61Jfn6cA+qHpyPYdTH+UshITnmp5/Ztkf
m/UTSLBNFNHesiTZeH31NcxYGdHSme9Nc/gfidRa0FLOCfWxRlFqAI47zG9jAQCZ
7Z2mCGDNMhjQc+BYcdnl0lPXjdDK6V0qCg1dVewhUBcW5gZKzV7e9+DpVA==
-----END
CERTIFICATE-----
HMAC_DRBG entropy usage SHA-1
depends_on:MBEDTLS_SHA1_C
hmac_drbg_entropy_usage:MBEDTLS_MD_SHA1

HMAC_DRBG entropy usage SHA-224
depends_on:MBEDTLS_SHA256_C
hmac_drbg_entropy_usage:MBEDTLS_MD_SHA224

HMAC_DRBG entropy usage SHA-256
depends_on:MBEDTLS_SHA256_C
hmac_drbg_entropy_usage:MBEDTLS_MD_SHA256

HMAC_DRBG entropy usage SHA-384
depends_on:MBEDTLS_SHA512_C
hmac_drbg_entropy_usage:MBEDTLS_MD_SHA384

HMAC_DRBG entropy usage SHA-512
depends_on:MBEDTLS_SHA512_C
hmac_drbg_entropy_usage:MBEDTLS_MD_SHA512

HMAC_DRBG write/update seed file SHA-1
depends_on:MBEDTLS_SHA1_C
hmac_drbg_seed_file:MBEDTLS_MD_SHA1:"data_files/hmac_drbg_seed":0

HMAC_DRBG write/update seed file SHA-1
depends_on:MBEDTLS_SHA1_C
hmac_drbg_seed_file:MBEDTLS_MD_SHA1:"no_such_dir/file":MBEDTLS_ERR_HMAC_DRBG_FILE_IO_ERROR

HMAC_DRBG write/update seed file SHA-224

depends_on:MBEDTLS_SHA256_C
hmac_drbg_seed_file:MBEDTLS_MD_SHA224:"data_files/hmac_drbg_seed":0

HMAC_DRBG write/update seed file SHA-224
depends_on:MBEDTLS_SHA256_C
hmac_drbg_seed_file:MBEDTLS_MD_SHA224:"no_such_dir/file":MBEDTLS_ERR_HMAC_DRBG_FILE_IO_ERROR

HMAC_DRBG
write/update seed file SHA-256
depends_on:MBEDTLS_SHA256_C
hmac_drbg_seed_file:MBEDTLS_MD_SHA256:"data_files/hmac_drbg_seed":0

HMAC_DRBG write/update seed file SHA-256
depends_on:MBEDTLS_SHA256_C
hmac_drbg_seed_file:MBEDTLS_MD_SHA256:"no_such_dir/file":MBEDTLS_ERR_HMAC_DRBG_FILE_IO_ERROR

HMAC_DRBG write/update seed file SHA-384
depends_on:MBEDTLS_SHA512_C
hmac_drbg_seed_file:MBEDTLS_MD_SHA384:"data_files/hmac_drbg_seed":0

HMAC_DRBG write/update seed file SHA-384
depends_on:MBEDTLS_SHA512_C
hmac_drbg_seed_file:MBEDTLS_MD_SHA384:"no_such_dir/file":MBEDTLS_ERR_HMAC_DRBG_FILE_IO_ERROR

HMAC_DRBG write/update seed file SHA-512
depends_on:MBEDTLS_SHA512_C
hmac_drbg_seed_file:MBEDTLS_MD_SHA512:"data_files/hmac_drbg_seed":0

HMAC_DRBG write/update seed file SHA-512
depends_on:MBEDTLS_SHA512_C
hmac_drbg_seed_file:MBEDTLS_MD_SHA512:"no_such_dir/file":MBEDTLS_ERR_HMAC_DRBG_FILE_IO_ERROR

HMAC_DRBG
from buffer SHA-1
depends_on:MBEDTLS_SHA1_C
hmac_drbg_buf:MBEDTLS_MD_SHA1

HMAC_DRBG from buffer SHA-224
depends_on:MBEDTLS_SHA256_C
hmac_drbg_buf:MBEDTLS_MD_SHA224

HMAC_DRBG from buffer SHA-256
depends_on:MBEDTLS_SHA256_C
hmac_drbg_buf:MBEDTLS_MD_SHA256

HMAC_DRBG from buffer SHA-384
depends_on:MBEDTLS_SHA512_C
hmac_drbg_buf:MBEDTLS_MD_SHA384

HMAC_DRBG from buffer SHA-512
depends_on:MBEDTLS_SHA512_C
hmac_drbg_buf:MBEDTLS_MD_SHA512

HMAC_DRBG self test
hmac_drbg_selftest:
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 6 (0x6)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=NL, O=PolarSSL, CN=PolarSSL Test CA
    Validity
      Not Before: Feb 12 14:44:07 2011 GMT
      Not After : Feb 12 14:44:07 2021 GMT
    Subject: C=NL, O=PolarSSL, CN=PolarSSL Cert MD5
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (2048 bit)
        Modulus (2048 bit):
          00:b9:3c:4a:c5:c8:a3:8e:90:17:a4:9e:52:aa:71:
          75:26:61:80:e7:c7:b5:6d:8c:ff:aa:b6:41:26:b7:
          be:11:ad:5c:73:16:0c:64:11:48:04:ff:d6:e1:3b:
          05:db:89:bb:b3:97:09:d5:1c:14:dd:68:87:39:b0:
          3d:71:cb:e2:76:d0:1a:d8:18:2d:80:1b:54:f6:e5:
          44:9a:f1:cb:af:61:2e:df:49:0d:9d:09:b7:ed:b1:
          fd:3c:fd:3c:fa:24:cf:5d:bf:7c:e4:53:e7:25:b5:
          ea:44:22:e9:26:d3:ea:20:94:9e:e6:61:67:ba:2e:
          07:67:0b:03:2f:a2:09:ed:f0:33:8f:0b:ce:10:ef:
          67:a4:c6:08:da:c1:ed:c2:3f:d7:4a:dd:15:3d:f9:
          5e:1c:81:60:46:3e:b5:b3:3d:2f:a6:de:47:1c:bc:
          92:ae:eb:df:27:6b:16:56:b7:dc:ec:d1:55:57:a5:
          6e:ec:75:25:f5:b7:7b:df:ab:d2:3a:5a:91:98:7d:
          97:17:0b:13:0a:a7:6b:4a:8b:c1:47:30:fb:3a:f8:
          41:04:d5:c1:df:b8:1d:bf:7b:01:a5:65:a2:e0:1e:
          36:b7:a6:5c:cc:30:5a:f8:cd:6f:cd:f1:19:62:25:
          ca:01:e3:35:7f:fa:20:f5:dc:fd:69:b2:6a:00:7d:
          17:f7
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints:
        CA:FALSE
      X509v3 Subject Key Identifier:

7D:E4:9C:6B:E6:F9:71:7D:46:D2:12:3D:AD:6B:1D:FD:C2:AA:78:4C
X509v3 Authority Key Identifier:
keyid:B4:5A:E4:A5:B3:DE:D2:52:F6:B9:D5:A6:95:0F:EB:3E:BC:C7:FD:FF

Signature Algorithm: md5WithRSAEncryption
92:13:81:0c:ff:ac:ab:98:52:6c:28:c9:c6:3e:80:c6:ec:77:
d0:13:e1:a2:29:1d:2f:b7:c5:95:41:83:60:d9:50:9c:d0:d6:
09:f7:0f:97:cd:c0:e6:b2:68:fa:31:c9:2a:a3:d3:1e:53:ae:
79:dc:35:ba:b0:d9:e5:7a:37:1b:2a:92:fa:d2:59:90:43:1b:
6a:91:c1:db:36:da:e9:39:d3:f5:ac:e3:46:01:ca:55:04:17:
1a:b1:97:28:e8:ff:1b:e7:e1:10:c9:b5:31:d8:ce:a6:89:6a:
4a:df:78:7b:02:2f:83:b3:41:d5:ef:0b:b6:44:ff:32:a6:cf:
1b:c2:f4:b0:75:66:a9:da:6f:7c:a5:e3:c6:c1:3a:2f:bf:f8:
12:6f:04:2c:37:f2:4e:fc:b9:09:ff:a4:5b:40:19:e9:58:91:
64:82:d6:ad:b9:7f:c0:12:c2:ce:b7:b6:ba:fb:10:a2:3f:74:
97:10:39:d4:dc:4a:e5:5c:f7:e5:3a:d9:68:d7:17:6b:f5:51:
08:b4:a2:30:0d:cc:36:10:6d:4e:1d:22:cc:48:d1:38:44:ba:
cc:2b:47:99:f7:c6:8b:41:24:f3:f1:2c:10:1a:f2:88:bb:b2:
e0:fd:44:26:3d:ad:ea:af:1d:d0:00:56:41:4e:f4:b0:3b:9d:
32:6f:48:c7
-----BEGIN CERTIFICATE-----
MIIDPzCCAiegAwIBAgIBBjANBgkqhkiG9w0BAQQFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTEwMjEyMTQ0NDA3WhcNMjEwMjEyMTQ0NDA3WjA8MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxGjAYBgNVBAMTEVBvbGFyU1NMIENlcnQgTUQ1MIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuTxKxcijjpAXpJ5SqnF1JmGA58e1
bYz/qrZBJre+Ea1ccxYMZBFIBP/W4TsF24m7s5cJ1RwU3WiHObA9ccvidtAa2Bgt
gBtU9uVEmvHLr2Eu30kNnQm37bH9PP08+iTPXb985FPnJbXqRCLpJtPqIJSe5mFn
ui4HZwsDL6IJ7fAzjwvOEO9npMYI2sHtwj/XSt0VPfleHIFgRj61sz0vpt5HHLyS
ruvfJ2sWVrfc7NFVV6Vu7HUl9bd736vSOlqRmH2XFwsTCqdrSovBRzD7OvhBBNXB
37gdv3sBpWWi4B42t6ZczDBa+M1vzfEZYiXKAeM1f/og9dz9abJqAH0X9wIDAQAB
o00wSzAJBgNVHRMEAjAAMB0GA1UdDgQWBBR95Jxr5vlxfUbSEj2tax39wqp4TDAf
BgNVHSMEGDAWgBS0WuSls97SUva51aaVD+s+vMf9/zANBgkqhkiG9w0BAQQFAAOC
AQEAkhOBDP+sq5hSbCjJxj6Axux30BPhoikdL7fFlUGDYNlQnNDWCfcPl83A5rJo
+jHJKqPTHlOuedw1urDZ5Xo3GyqS+tJZkEMbapHB2zba6TnT9azjRgHKVQQXGrGX
KOj/G+fhEMm1MdjOpolqSt94ewIvg7NB1e8LtkT/MqbPG8L0sHVmqdpvfKXjxsE6
L7/4Em8ELDfyTvy5Cf+kW0AZ6ViRZILWrbl/wBLCzre2uvsQoj90lxA51NxK5Vz3
5TrZaNcXa/VRCLSiMA3MNhBtTh0izEjROES6zCtHmffGi0Ek8/EsEBryiLuy4P1E
Jj2t6q8d0ABWQU70sDudMm9Ixw==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE REQUEST-----
MIIBGDCBvwIBADA0MQswCQYDVQQGEwJOTDERMA8GA1UEChMIUG9sYXJTU0wxEjAQ
BgNVBAMTCWxvY2FsaG9zdDBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABDfMVtl2
CR5acj7HWS3/IG7ufPkGkXTQrRS192giWWKSTuUA2CMR/+ov0jRdXRa9iojCa3cN
Vc2KKg76Aci07f+gKTAnBgkqhkiG9w0BCQ4xGjAYMAkGA1UdEwQCMAAwCwYDVR0P
BAQDAgXgMAoGCCqGSM49BAMEA0gAMEUCIQD8xdtluTiBJM50d/WvDeUvPbXOUMlL
8xEJXU2WOK+RLAIgS8U6Z8tlJpXLEisz/j4gdABG3Y3h4PBJjlpszFisTNo=

-----END CERTIFICATE REQUEST-----
Decrypt empty buffer
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
dec_empty_buf:

AES Encrypt and decrypt 0 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:0:-1

AES Encrypt and decrypt 1 byte
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:1:-1

AES Encrypt and decrypt 2 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:2:-1

AES Encrypt and decrypt 7 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:7:-1

AES Encrypt and decrypt 8 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:8:-1

AES Encrypt and decrypt
9 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:9:-1

AES Encrypt and decrypt 15 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:15:-1

AES Encrypt and decrypt 16 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:16:-1

AES Encrypt and decrypt 17 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:17:-1

AES Encrypt and decrypt 31 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:31:-1

AES Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7

enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:32:-1

AES
Encrypt and decrypt 33 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:33:-1

AES Encrypt and decrypt 47 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:47:-1

AES Encrypt and decrypt 48 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:48:-1

AES Encrypt and decrypt 49 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:49:-1

AES Encrypt and decrypt 0 bytes with one and zeros padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ONE_AND_ZEROS
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:0:MBEDTLS_PADDING_ONE_AND_ZEROS

AES Encrypt and decrypt 1 byte with one
and zeros padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ONE_AND_ZEROS
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:1:MBEDTLS_PADDING_ONE_AND_ZEROS

AES Encrypt and decrypt 2 bytes with one and zeros padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ONE_AND_ZEROS
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:2:MBEDTLS_PADDING_ONE_AND_ZEROS

AES Encrypt and decrypt 7 bytes with one and zeros padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ONE_AND_ZEROS
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:7:MBEDTLS_PADDING_ONE_AND_ZEROS

AES Encrypt and decrypt 8 bytes with one and zeros padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ONE_AND_ZEROS
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-

CBC":128:8:MBEDTLS_PADDING_ONE_AND_ZEROS

AES Encrypt and decrypt 9 bytes with one and zeros padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ONE_AN
D_ZEROS
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-
CBC":128:9:MBEDTLS_PADDING_ONE_AND_ZEROS

AES
Encrypt and decrypt 15 bytes with one and zeros padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ONE_AN
D_ZEROS
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-
CBC":128:15:MBEDTLS_PADDING_ONE_AND_ZEROS

AES Encrypt and decrypt 16 bytes with one and zeros padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ONE_AN
D_ZEROS
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-
CBC":128:16:MBEDTLS_PADDING_ONE_AND_ZEROS

AES Encrypt and decrypt 17 bytes with one and zeros padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ONE_AN
D_ZEROS
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-
CBC":128:17:MBEDTLS_PADDING_ONE_AND_ZEROS

AES Encrypt and decrypt 31 bytes with one and zeros padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ONE_AN
D_ZEROS
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-
CBC":128:31:MBEDTLS_PADDING_ONE_AND_ZEROS

AES
Encrypt and decrypt 32 bytes with one and zeros padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ONE_AN
D_ZEROS
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-
CBC":128:32:MBEDTLS_PADDING_ONE_AND_ZEROS

AES Encrypt and decrypt 33 bytes with one and zeros padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ONE_AN
D_ZEROS
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-
CBC":128:33:MBEDTLS_PADDING_ONE_AND_ZEROS

AES Encrypt and decrypt 47 bytes with one and zeros padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ONE_AN

D_ZEROS
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-
CBC":128:47:MBEDTLS_PADDING_ONE_AND_ZEROS

AES Encrypt and decrypt 48 bytes with one and zeros padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ONE_AN
D_ZEROS
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-
CBC":128:48:MBEDTLS_PADDING_ONE_AND_ZEROS

AES
Encrypt and decrypt 49 bytes with one and zeros padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ONE_AN
D_ZEROS
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-
CBC":128:49:MBEDTLS_PADDING_ONE_AND_ZEROS

AES Encrypt and decrypt 0 bytes with zeros and len padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ZEROS_
AND_LEN
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-
CBC":128:0:MBEDTLS_PADDING_ZEROS_AND_LEN

AES Encrypt and decrypt 1 byte with zeros and len padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ZEROS_
AND_LEN
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-
CBC":128:1:MBEDTLS_PADDING_ZEROS_AND_LEN

AES Encrypt and decrypt 2 bytes with zeros and len padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ZEROS_
AND_LEN
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-
CBC":128:2:MBEDTLS_PADDING_ZEROS_AND_LEN

AES Encrypt and decrypt 7 bytes
with zeros and len padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ZEROS_
AND_LEN
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-
CBC":128:7:MBEDTLS_PADDING_ZEROS_AND_LEN

AES Encrypt and decrypt 8 bytes with zeros and len padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ZEROS_
AND_LEN
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-
CBC":128:8:MBEDTLS_PADDING_ZEROS_AND_LEN

AES Encrypt and decrypt 9 bytes with zeros and len padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ZEROS_AND_LEN
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:9:MBEDTLS_PADDING_ZEROS_AND_LEN

AES Encrypt and decrypt 15 bytes with zeros and len padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ZEROS_AND_LEN
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:15:MBEDTLS_PADDING_ZEROS_AND_LEN

AES Encrypt and decrypt 16 bytes with zeros and len padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ZEROS_AND_LEN
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:16:MBEDTLS_PADDING_ZEROS_AND_LEN

AES
Encrypt and decrypt 17 bytes with zeros and len padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ZEROS_AND_LEN
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:17:MBEDTLS_PADDING_ZEROS_AND_LEN

AES Encrypt and decrypt 31 bytes with zeros and len padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ZEROS_AND_LEN
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:31:MBEDTLS_PADDING_ZEROS_AND_LEN

AES Encrypt and decrypt 32 bytes with zeros and len padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ZEROS_AND_LEN
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:32:MBEDTLS_PADDING_ZEROS_AND_LEN

AES Encrypt and decrypt 33 bytes with zeros and len padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ZEROS_AND_LEN
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:33:MBEDTLS_PADDING_ZEROS_AND_LEN

AES
Encrypt and decrypt 47 bytes with zeros and len padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ZEROS_AND_LEN
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-

CBC":128:47:MBEDTLS_PADDING_ZEROS_AND_LEN

AES Encrypt and decrypt 48 bytes with zeros and len padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ZEROS_AND_LEN
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:48:MBEDTLS_PADDING_ZEROS_AND_LEN

AES Encrypt and decrypt 49 bytes with zeros and len padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ZEROS_AND_LEN
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:49:MBEDTLS_PADDING_ZEROS_AND_LEN

AES Encrypt and decrypt 0 bytes with zeros padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ZEROS
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:0:MBEDTLS_PADDING_ZEROS

AES
Encrypt and decrypt 1 byte with zeros padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ZEROS
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:1:MBEDTLS_PADDING_ZEROS

AES Encrypt and decrypt 2 bytes with zeros padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ZEROS
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:2:MBEDTLS_PADDING_ZEROS

AES Encrypt and decrypt 7 bytes with zeros padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ZEROS
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:7:MBEDTLS_PADDING_ZEROS

AES Encrypt and decrypt 8 bytes with zeros padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ZEROS
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:8:MBEDTLS_PADDING_ZEROS

AES Encrypt and decrypt 9 bytes with zeros padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ZEROS
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:9:MBEDTLS_PADDING_ZEROS

AES
Encrypt and decrypt 15 bytes with zeros padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ZEROS
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:15:MBEDTLS_PADDING_ZEROS

AES Encrypt and decrypt 16 bytes with zeros padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ZEROS
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:16:MBEDTLS_PADDING_ZEROS

AES Encrypt and decrypt 17 bytes with zeros padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ZEROS
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:17:MBEDTLS_PADDING_ZEROS

AES Encrypt and decrypt 31 bytes with zeros padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ZEROS
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:31:MBEDTLS_PADDING_ZEROS

AES Encrypt and decrypt 32 bytes with zeros padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ZEROS
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:32:MBEDTLS_PADDING_ZEROS

AES
Encrypt and decrypt 33 bytes with zeros padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ZEROS
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:33:MBEDTLS_PADDING_ZEROS

AES Encrypt and decrypt 47 bytes with zeros padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ZEROS
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:47:MBEDTLS_PADDING_ZEROS

AES Encrypt and decrypt 48 bytes with zeros padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ZEROS
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:48:MBEDTLS_PADDING_ZEROS

AES Encrypt and decrypt 49 bytes with zeros padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_ZEROS
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:49:MBEDTLS_PADDING_ZEROS

AES Encrypt
and decrypt 0 bytes with no padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:0:MBEDTLS_PADDING_NONE

AES Encrypt and decrypt 16 bytes with no padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:16:MBEDTLS_PADDING_NONE

AES Encrypt and decrypt 32 bytes with no padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:32:MBEDTLS_PADDING_NONE

AES Encrypt and decrypt 48 bytes with no padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CBC:"AES-128-CBC":128:48:MBEDTLS_PADDING_NONE

AES Try encrypting 1 bytes with no padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7

enc_fail:MBEDTLS_CIPHER_AES_128_CBC:MBEDTLS_PADDING_NONE:128:1:MBEDTLS_ERR_CIPHER_FULL_BLOCK_EXPECTED

AES
Try encrypting 2 bytes with no padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_AES_128_CBC:MBEDTLS_PADDING_NONE:128:2:MBEDTLS_ERR_CIPHER_FULL_BLOCK_EXPECTED

AES Try encrypting 7 bytes with no padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_AES_128_CBC:MBEDTLS_PADDING_NONE:128:7:MBEDTLS_ERR_CIPHER_FULL_BLOCK_EXPECTED

AES Try encrypting 8 bytes with no padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_AES_128_CBC:MBEDTLS_PADDING_NONE:128:8:MBEDTLS_ERR_CIPHER_FULL_BLOCK_EXPECTED

AES Try encrypting 9 bytes with no padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_AES_128_CBC:MBEDTLS_PADDING_NONE:128:9:MBEDTLS_ERR_CIPHER_FULL_BLOCK_EXPECTED

AES Try encrypting 15 bytes with no padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_AES_128_CBC:MBEDTLS_PADDING_NONE:128:15:MBEDTLS_ERR_CIPHER_FULL_BLOCK_EXPECTED

AES
Try encrypting 17 bytes with no padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_AES_128_CBC:MBEDTLS_PADDING_NONE:128:17:MBEDTLS_ERR_CIPHER_FULL_BLOCK_EXPECTED

AES Try encrypting 31 bytes with no padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_AES_128_CBC:MBEDTLS_PADDING_NONE:128:31:MBEDTLS_ERR_CIPHER_FULL_BLOCK_EXPECTED

AES Try encrypting 33 bytes with no padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_AES_128_CBC:MBEDTLS_PADDING_NONE:128:33:MBEDTLS_ERR_CIPHER_FULL_BLOCK_EXPECTED

AES Try encrypting 47 bytes with no padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_AES_128_CBC:MBEDTLS_PADDING_NONE:128:47:MBEDTLS_ERR_CIPHE

R_FULL_BLOCK_EXPECTED

AES
Try encrypting 49 bytes with no padding
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_AES_128_CBC:MBEDTLS_PADDING_NONE:128:49:MBEDTLS_ERR_CIPHE
R_FULL_BLOCK_EXPECTED

AES Encrypt and decrypt 0 bytes in multiple parts
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CBC:128:0:0:

AES Encrypt and decrypt 1 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CBC:128:1:0:

AES Encrypt and decrypt 1 bytes in multiple parts 2
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CBC:128:0:1:

AES Encrypt and decrypt 16 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CBC:128:16:0:

AES
Encrypt and decrypt 16 bytes in multiple parts 2
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CBC:128:0:16:

AES Encrypt and decrypt 16 bytes in multiple parts 3
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CBC:128:1:15:

AES Encrypt and decrypt 16 bytes in multiple parts 4
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CBC:128:15:1:

AES Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CBC:128:15:7:

AES Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CBC:128:16:6:

AES
Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7

enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CBC:128:17:6:

AES Encrypt and decrypt 32 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CBC:128:16:16:

AES Encrypt and decrypt 0 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CFB128:"AES-128-CFB128":128:0:-1

AES Encrypt and decrypt 1 byte
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CFB128:"AES-128-CFB128":128:1:-1

AES Encrypt and decrypt 2 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CFB128:"AES-128-CFB128":128:2:-1

AES Encrypt and decrypt 7 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CFB128:"AES-128-CFB128":128:7:-1

AES Encrypt
and decrypt 8 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CFB128:"AES-128-CFB128":128:8:-1

AES Encrypt and decrypt 9 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CFB128:"AES-128-CFB128":128:9:-1

AES Encrypt and decrypt 15 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CFB128:"AES-128-CFB128":128:15:-1

AES Encrypt and decrypt 16 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CFB128:"AES-128-CFB128":128:16:-1

AES Encrypt and decrypt 17 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CFB128:"AES-128-CFB128":128:17:-1

AES Encrypt and decrypt 31 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CFB128:"AES-128-CFB128":128:31:-1

AES Encrypt and decrypt 32 bytes

depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CFB128:"AES-128-CFB128":128:32:-1

AES
Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CFB128:"AES-128-CFB128":128:33:-1

AES Encrypt and decrypt 47 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CFB128:"AES-128-CFB128":128:47:-1

AES Encrypt and decrypt 48 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CFB128:"AES-128-CFB128":128:48:-1

AES Encrypt and decrypt 49 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CFB128:"AES-128-CFB128":128:49:-1

AES Encrypt and decrypt 0 bytes in multiple parts
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CFB128:128:0:0:

AES Encrypt and decrypt 1 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CFB128:128:1:0:

AES Encrypt and
decrypt 1 bytes in multiple parts 2
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CFB128:128:0:1:

AES Encrypt and decrypt 16 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CFB128:128:16:0:

AES Encrypt and decrypt 16 bytes in multiple parts 2
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CFB128:128:0:16:

AES Encrypt and decrypt 16 bytes in multiple parts 3
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CFB128:128:1:15:

AES Encrypt and decrypt 16 bytes in multiple parts 4
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CFB128:128:15:1:

AES Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CFB128:128:15:7:

AES Encrypt and decrypt 22
bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CFB128:128:16:6:

AES Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CFB128:128:17:6:

AES Encrypt and decrypt 32 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CFB128:128:16:16:

AES Encrypt and decrypt 0 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CTR:"AES-128-CTR":128:0:-1

AES Encrypt and decrypt 1 byte
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CTR:"AES-128-CTR":128:1:-1

AES Encrypt and decrypt 2 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CTR:"AES-128-CTR":128:2:-1

AES Encrypt and decrypt 7 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CTR:"AES-128-CTR":128:7:-1

AES
Encrypt and decrypt 8 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CTR:"AES-128-CTR":128:8:-1

AES Encrypt and decrypt 9 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CTR:"AES-128-CTR":128:9:-1

AES Encrypt and decrypt 15 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CTR:"AES-128-CTR":128:15:-1

AES Encrypt and decrypt 16 bytes

depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CTR:"AES-128-CTR":128:16:-1

AES Encrypt and decrypt 17 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CTR:"AES-128-CTR":128:17:-1

AES Encrypt and decrypt 31 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CTR:"AES-128-CTR":128:31:-1

AES Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CTR:"AES-128-CTR":128:32:-1

AES
Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CTR:"AES-128-CTR":128:33:-1

AES Encrypt and decrypt 47 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CTR:"AES-128-CTR":128:47:-1

AES Encrypt and decrypt 48 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CTR:"AES-128-CTR":128:48:-1

AES Encrypt and decrypt 49 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_AES_128_CTR:"AES-128-CTR":128:49:-1

AES Encrypt and decrypt 0 bytes in multiple parts
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CTR:128:0:0:

AES Encrypt and decrypt 1 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CTR:128:1:0:

AES Encrypt and decrypt 1 bytes in
multiple parts 2
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CTR:128:0:1:

AES Encrypt and decrypt 16 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CTR:128:16:0:

AES Encrypt and decrypt 16 bytes in multiple parts 2
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CTR:128:0:16:

AES Encrypt and decrypt 16 bytes in multiple parts 3
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CTR:128:1:15:

AES Encrypt and decrypt 16 bytes in multiple parts 4
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CTR:128:15:1:

AES Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CTR:128:15:7:

AES Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CTR:128:16:6:

AES
Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CTR:128:17:6:

AES Encrypt and decrypt 32 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_128_CTR:128:16:16:

AES Encrypt and decrypt 0 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_192_CBC:"AES-192-CBC":192:0:-1

AES Encrypt and decrypt 1 byte
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_192_CBC:"AES-192-CBC":192:1:-1

AES Encrypt and decrypt 2 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_192_CBC:"AES-192-CBC":192:2:-1

AES Encrypt and decrypt 7 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_192_CBC:"AES-192-CBC":192:7:-1

AES

Encrypt and decrypt 8 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_192_CBC:"AES-192-CBC":192:8:-1

AES Encrypt and decrypt 9 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_192_CBC:"AES-192-CBC":192:9:-1

AES Encrypt and decrypt 15 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_192_CBC:"AES-192-CBC":192:15:-1

AES Encrypt and decrypt 16 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_192_CBC:"AES-192-CBC":192:16:-1

AES Encrypt and decrypt 17 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_192_CBC:"AES-192-CBC":192:17:-1

AES Encrypt and
decrypt 31 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_192_CBC:"AES-192-CBC":192:31:-1

AES Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_192_CBC:"AES-192-CBC":192:32:-1

AES Encrypt and decrypt 33 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_192_CBC:"AES-192-CBC":192:33:-1

AES Encrypt and decrypt 47 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_192_CBC:"AES-192-CBC":192:47:-1

AES Encrypt and decrypt 48 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_192_CBC:"AES-192-CBC":192:48:-1

AES Encrypt and decrypt 49 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_192_CBC:"AES-192-CBC":192:49:-1

AES
Encrypt and decrypt 0 bytes in multiple parts
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7

enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_192_CBC:192:0:0:

AES Encrypt and decrypt 1 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_192_CBC:192:1:0:

AES Encrypt and decrypt 1 bytes in multiple parts 2
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_192_CBC:192:0:1:

AES Encrypt and decrypt 16 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_192_CBC:192:16:0:

AES Encrypt and decrypt 16 bytes in multiple parts 2
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_192_CBC:192:0:16:

AES Encrypt and decrypt
16 bytes in multiple parts 3
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_192_CBC:192:1:15:

AES Encrypt and decrypt 16 bytes in multiple parts 4
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_192_CBC:192:15:1:

AES Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_192_CBC:192:15:7:

AES Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_192_CBC:192:16:6:

AES Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_192_CBC:192:17:6:

AES Encrypt and decrypt 32 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_192_CBC:192:16:16:

AES
Encrypt and decrypt 0 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_256_CBC:"AES-256-CBC":256:0:-1

AES Encrypt and decrypt 1 byte
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_256_CBC:"AES-256-CBC":256:1:-1

AES Encrypt and decrypt 2 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_256_CBC:"AES-256-CBC":256:2:-1

AES Encrypt and decrypt 7 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_256_CBC:"AES-256-CBC":256:7:-1

AES Encrypt and decrypt 8 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_256_CBC:"AES-256-CBC":256:8:-1

AES Encrypt
and decrypt 9 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_256_CBC:"AES-256-CBC":256:9:-1

AES Encrypt and decrypt 15 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_256_CBC:"AES-256-CBC":256:15:-1

AES Encrypt and decrypt 16 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_256_CBC:"AES-256-CBC":256:16:-1

AES Encrypt and decrypt 17 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_256_CBC:"AES-256-CBC":256:17:-1

AES Encrypt and decrypt 31 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_256_CBC:"AES-256-CBC":256:31:-1

AES Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_256_CBC:"AES-256-CBC":256:32:-1

AES
Encrypt and decrypt 33 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_256_CBC:"AES-256-CBC":256:33:-1

AES Encrypt and decrypt 47 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7

enc_dec_buf:MBEDTLS_CIPHER_AES_256_CBC:"AES-256-CBC":256:47:-1

AES Encrypt and decrypt 48 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_256_CBC:"AES-256-CBC":256:48:-1

AES Encrypt and decrypt 49 bytes
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_AES_256_CBC:"AES-256-CBC":256:49:-1

AES Encrypt and decrypt 0 bytes in multiple parts
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_256_CBC:256:0:0:

AES Encrypt and decrypt 1 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_256_CBC:256:1:0:

AES
Encrypt and decrypt 1 bytes in multiple parts 2
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_256_CBC:256:0:1:

AES Encrypt and decrypt 16 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_256_CBC:256:16:0:

AES Encrypt and decrypt 16 bytes in multiple parts 2
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_256_CBC:256:0:16:

AES Encrypt and decrypt 16 bytes in multiple parts 3
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_256_CBC:256:1:15:

AES Encrypt and decrypt 16 bytes in multiple parts 4
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_256_CBC:256:15:1:

AES
Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_256_CBC:256:15:7:

AES Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_256_CBC:256:16:6:

AES Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_256_CBC:256:17:6:

AES Encrypt and decrypt 32 bytes in multiple parts 1
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_AES_256_CBC:256:16:16:

AES Decrypt test vector #0
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_PADDING_PKCS7:MBEDTLS_CIPHER_MODE_CBC:
MBEDTLS_CIPHER_PADDING_PKCS7
decrypt_test_vec:MBEDTLS_CIPHER_AES_128_CBC:MBEDTLS_PADDING_PKCS7:"fffffffe0000000000000
0000000000":"00000000000000000000000000000000":"23f710842b9bb9c32f26648c786807ca":"00000000000000
000000000000000000":"":"":MBEDTLS_ERR_CIPHER_INVALID_PADDING:0

AES
Decrypt test vector #1
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
decrypt_test_vec:MBEDTLS_CIPHER_AES_128_CBC:MBEDTLS_PADDING_NONE:"ffffffffe00000000000000
000000000":"00000000000000000000000000000000":"23f710842b9bb9c32f26648c786807ca":"00000000000000
000000000000000000":"":"":0:0

AES Decrypt test vector #2
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
decrypt_test_vec:MBEDTLS_CIPHER_AES_192_CBC:MBEDTLS_PADDING_NONE:"00000000000000000000
0000000000000000000000000000":"00000000000000000000000000000000":"707b1dbb0ffa40ef7d95def421233fa
e":"ffffffff800000000000000000000000":"":"":0:0

AES Decrypt test vector #3
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
decrypt_test_vec:MBEDTLS_CIPHER_AES_256_CBC:MBEDTLS_PADDING_NONE:"00000000000000000000
0000000000000000000000000000000000000000000000":"00000000000000000000000000000000":"49af6b372135a
cef10132e548f217b17":"ff000000000000000000000000000000":"":"":0:0

AES
Decrypt test vector #4
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CFB
decrypt_test_vec:MBEDTLS_CIPHER_AES_128_CFB128:-
1:"fffffffe00000000000000000000000":"00000000000000000000000000000000":"1114bc2028009b923f0b01915
ce5e7c4":"00000000000000000000000000000000":"":"":0:0:

AES Decrypt test vector #5
depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CFB
decrypt_test_vec:MBEDTLS_CIPHER_AES_192_CFB128:-
1:"fffffffffffffffffffffffffffffffffffffffffffe00000":"00000000000000000000000000000000":"60136703374f64e860b48
ce31f930716":"00000000000000000000000000000000":"":"":0:0

AES Decrypt test vector #6

depends_on:MBEDTLS_AES_C:MBEDTLS_CIPHER_MODE_CFB
decrypt_test_vec:MBEDTLS_CIPHER_AES_256_CFB128:-
1:"fffffffff8000000000000000000000000000000000000000000000000000000":"00000000000000000000000000000000":"be66cfea2fecd6bf0ec7b4352c99bcaa":"00000000000000000000000000000000":"":"":0:0

AES-128-ECB
Encrypt NIST KAT #1
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_128_ECB:MBEDTLS_ENCRYPT:"00000000000000000000000000000000":"f34481ec3cc627bacd5dc3fb08f273e6":"0336763e966d92595a567cc9ce537f5e":0

AES-128-ECB Encrypt NIST KAT #2
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_128_ECB:MBEDTLS_ENCRYPT:"00000000000000000000000000000000":"9798c4640bad75c7c3227db910174e72":"a9a1631bf4996954ebc093957b234589":0

AES-128-ECB Encrypt NIST KAT #3
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_128_ECB:MBEDTLS_ENCRYPT:"00000000000000000000000000000000":"96ab5c2ff612d9dfaae8c31f30c42168":"ff4f8391a6a40ca5b25d23bedd44a597":0

AES-128-ECB Encrypt NIST KAT #4
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_128_ECB:MBEDTLS_ENCRYPT:"e0000000000000000000000000000000":"00000000000000000000000000000000":"72a1da770f5d7ac4c9ef94d822affd97":0

AES-128-ECB
Encrypt NIST KAT #5
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_128_ECB:MBEDTLS_ENCRYPT:"f0000000000000000000000000000000":"00000000000000000000000000000000":"970014d634e2b7650777e8e84d03ccd8":0

AES-128-ECB Encrypt NIST KAT #6
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_128_ECB:MBEDTLS_ENCRYPT:"f8000000000000000000000000000000":"00000000000000000000000000000000":"f17e79aed0db7e279e955b5f493875a7":0

AES-128-ECB Encrypt NIST KAT #7
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_128_ECB:MBEDTLS_ENCRYPT:"fffffffffffff000000000000000000":"00000000000000000000000000000000":"7b90785125505fad59b13c186dd66ce3":0

AES-128-ECB Encrypt NIST KAT #8
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_128_ECB:MBEDTLS_ENCRYPT:"fffffffffffff800000000000000000":"00000000000000000000000000000000":"8b527a6aebdaec9eaef8eda2cb7783e5":0

AES-128-ECB Encrypt NIST KAT #9

depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_128_ECB:MBEDTLS_ENCRYPT:"fffffffffffffc00000000000000000":"
00000000000000000000000000000000":"43fdaf53ebbc9880c228617d6a9b548b":0

AES-128-ECB
Encrypt NIST KAT #10
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_128_ECB:MBEDTLS_ENCRYPT:"fffffffffffffffffffffffffffc000":"00000
000000000000000000000000000":"70c46bb30692be657f7eaa93ebad9897":0

AES-128-ECB Encrypt NIST KAT #11
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_128_ECB:MBEDTLS_ENCRYPT:"fffffffffffffffffffffffffffe000":"00000
000000000000000000000000000":"323994cfb9da285a5d9642e1759b224a":0

AES-128-ECB Encrypt NIST KAT #12
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_128_ECB:MBEDTLS_ENCRYPT:"fffffffffffffffffffffffffffff000":"00000
000000000000000000000000000":"1dbf57877b7b17385c85d0b54851e371":0

AES-128-ECB Encrypt NIST KAT #13
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_128_ECB:MBEDTLS_ENCRYPT:"00000000000000000000000000000000
00":"fffffffffffffc00000000000000000":"3a4d354f02bb5a5e47d39666867f246a":0

AES-128-ECB Encrypt
NIST KAT #14
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_128_ECB:MBEDTLS_ENCRYPT:"00000000000000000000000000000000
00":"fffffffffffffe00000000000000000":"d451b8d6e1e1a0ebb155fbbf6e7b7dc3":0

AES-128-ECB Encrypt NIST KAT #15
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_128_ECB:MBEDTLS_ENCRYPT:"00000000000000000000000000000000
00":"ffffffffffffff00000000000000000":"6898d4f42fa7ba6a10ac05e87b9f2080":0

AES-128-ECB Encrypt NIST KAT #16
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_128_ECB:MBEDTLS_ENCRYPT:"00000000000000000000000000000000
00":"fffffffffffffffffffffffe0000000":"082eb8be35f442fb52668e16a591d1d6":0

AES-128-ECB Encrypt NIST KAT #17
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_128_ECB:MBEDTLS_ENCRYPT:"00000000000000000000000000000000
00":"ffffffffffffffffffffffff0000000":"e656f9ecf5fe27ec3e4a73d00c282fb3":0

AES-128-ECB Encrypt NIST KAT #18
depends_on:MBEDTLS_AES_C

test_vec_ecb:MBEDTLS_CIPHER_AES_128_ECB:MBEDTLS_ENCRYPT:"00000000000000000000000000000000":"ffffffffffffffffffffffff8000000":"2ca8209d63274cd9a29bb74bcd77683a":0

AES-128-ECB
Decrypt NIST KAT #1
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_128_ECB:MBEDTLS_DECRYPT:"00000000000000000000000000000000":"db4f1aa530967d6732ce4715eb0ee24b":"ff000000000000000000000000000000":0

AES-128-ECB Decrypt NIST KAT #2
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_128_ECB:MBEDTLS_DECRYPT:"00000000000000000000000000000000":"a81738252621dd180a34f3455b4baa2f":"ff800000000000000000000000000000":0

AES-128-ECB Decrypt NIST KAT #3
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_128_ECB:MBEDTLS_DECRYPT:"00000000000000000000000000000000":"77e2b508db7fd89234caf7939ee5621a":"ffc00000000000000000000000000000":0

AES-128-ECB Decrypt NIST KAT #4
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_128_ECB:MBEDTLS_DECRYPT:"00000000000000000000000000000000":"dc43be40be0e53712f7e2bf5ca707209":"6a118a874519e64e9963798a503f1d35":0

AES-128-ECB Decrypt
NIST KAT #5
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_128_ECB:MBEDTLS_DECRYPT:"00000000000000000000000000000000":"92beedab1895a94faa69b632e5cc47ce":"cb9fceec81286ca3e989bd979b0cb284":0

AES-128-ECB Decrypt NIST KAT #6
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_128_ECB:MBEDTLS_DECRYPT:"00000000000000000000000000000000":"459264f4798f6a78bacb89c15ed3d601":"b26aeb1874e47ca8358ff22378f09144":0

AES-128-ECB Decrypt NIST KAT #7
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_128_ECB:MBEDTLS_DECRYPT:"b69418a85332240dc82492353956ae0c":"a303d940ded8f0baff6f75414cac5243":"00000000000000000000000000000000":0

AES-128-ECB Decrypt NIST KAT #8
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_128_ECB:MBEDTLS_DECRYPT:"71b5c08a1993e1362e4d0ce9b22b78d5":"c2dabd117f8a3ecabfbb11d12194d9d0":"00000000000000000000000000000000":0

AES-128-ECB Decrypt NIST KAT #9
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_128_ECB:MBEDTLS_DECRYPT:"e234cdca2606b81f29408d5f6da2120

6":"fff60a4740086b3b9c56195b98d91a7b":"00000000000000000000000000000000":0

AES-128-ECB
Decrypt NIST KAT #10
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_128_ECB:MBEDTLS_DECRYPT:"ffffffffffffffff0000000000000000":"84be19e053635f09f2665e7bae85b42d":"00000000000000000000000000000000":0

AES-128-ECB Decrypt NIST KAT #11
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_128_ECB:MBEDTLS_DECRYPT:"ffffffffffffffff8000000000000000":"32cd652842926aea4aa6137bb2be2b5e":"00000000000000000000000000000000":0

AES-192-ECB Encrypt NIST KAT #1
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_192_ECB:MBEDTLS_ENCRYPT:"000000000000000000000000000000000000000000000000":"ffffffffffffffffffff80000000000":"156f07767a85a4312321f63968338a01":0

AES-192-ECB Encrypt NIST KAT #2
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_192_ECB:MBEDTLS_ENCRYPT:"000000000000000000000000000000000000000000000000":"ffffffffffffffffffffc0000000000":"15eec9ebf42b9ca76897d2cd6c5a12e2":0

AES-192-ECB
Encrypt NIST KAT #3
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_192_ECB:MBEDTLS_ENCRYPT:"000000000000000000000000000000000000000000000000":"ffffffffffffffffffffe0000000000":"db0d3a6fdcc13f915e2b302ceeb70fd8":0

AES-192-ECB Encrypt NIST KAT #4
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_192_ECB:MBEDTLS_ENCRYPT:"000000000000000000000000000000000000000000000000":"51719783d3185a535bd75adc65071ce1":"4f354592ff7c8847d2d0870ca9481b7c":0

AES-192-ECB Encrypt NIST KAT #5
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_192_ECB:MBEDTLS_ENCRYPT:"000000000000000000000000000000000000000000000000":"26aa49dcfe7629a8901a69a9914e6dfd":"d5e08bf9a182e857cf40b3a36ee248cc":0

AES-192-ECB Encrypt NIST KAT #6
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_192_ECB:MBEDTLS_ENCRYPT:"000000000000000000000000000000000000000000000000":"941a4773058224e1ef66d10e0a6ee782":"067cd9d3749207791841562507fa9626":0

AES-192-ECB Encrypt NIST KAT #7
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_192_ECB:MBEDTLS_ENCRYPT:"d2926527e0aa9f37b45e2ec2ade5853ef807576104c7ace3":"00000000000000000000000000000000":"dd619e1cf204446112e0af2b9afa8f8c":0

AES-192-ECB
Encrypt NIST KAT #8
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_192_ECB:MBEDTLS_ENCRYPT:"982215f4e173dfa0fcffe5d3da41c4812c7bcc8ed3540f93":"00000000000000000000000000000000":"d4f0aae13c8fe9339fbf9e69ed0ad74d":0

AES-192-ECB Encrypt NIST KAT #9
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_192_ECB:MBEDTLS_ENCRYPT:"98c6b8e01e379fbd14e61af6af891596583565f2a27d59e9":"00000000000000000000000000000000":"19c80ec4a6deb7e5ed1033dda933498f":0

AES-192-ECB Encrypt NIST KAT #10
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_192_ECB:MBEDTLS_ENCRYPT:"ffffffffffffffffffffffffff800000000000000000":"00000000000000000000000000000000":"8dd274bd0f1b58ae345d9e7233f9b8f3":0

AES-192-ECB Encrypt NIST KAT #11
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_192_ECB:MBEDTLS_ENCRYPT:"ffffffffffffffffffffffffffc000000000000000000":"00000000000000000000000000000000":"9d6bdc8f4ce5feb0f3bed2e4b9a9bb0b":0

AES-192-ECB
Encrypt NIST KAT #12
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_192_ECB:MBEDTLS_ENCRYPT:"ffffffffffffffffffffffffffe000000000000000000":"00000000000000000000000000000000":"fd5548bcf3f42565f7efa94562528d46":0

AES-192-ECB Decrypt NIST KAT #1
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_192_ECB:MBEDTLS_DECRYPT:"ffffffffffffffffffffffffffffff000000000000000":"bb2852c891c5947d2ed44032c421b85f":"00000000000000000000000000000000":0

AES-192-ECB Decrypt NIST KAT #2
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_192_ECB:MBEDTLS_DECRYPT:"ffffffffffffffffffffffffffffff800000000000000":"1b9f5fbd5e8a4264c0a85b80409afa5e":"00000000000000000000000000000000":0

AES-192-ECB Decrypt NIST KAT #3
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_192_ECB:MBEDTLS_DECRYPT:"ffffffffffffffffffffffffffffffc000000000000000":"30dab809f85a917fe924733f424ac589":"00000000000000000000000000000000":0

AES-192-ECB
Decrypt NIST KAT #4
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_192_ECB:MBEDTLS_DECRYPT:"61257134a518a0d57d9d244d45f6498cbc32f2bafc522d79":"cfe4d74002696ccf7d87b14a2f9cafc9":"00000000000000000000000000000000":0

AES-192-ECB Decrypt NIST KAT #5
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_192_ECB:MBEDTLS_DECRYPT:"b0ab0a6a818baef2d11fa33eac94728
4fb7d748cfb75e570":"d2eafd86f63b109b91f5dbb3a3fb7e13":"00000000000000000000000000000000":0

AES-192-ECB Decrypt NIST KAT #6
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_192_ECB:MBEDTLS_DECRYPT:"ee053aa011c8b428cdcc3636313c54d
6a03cac01c71579d6":"9b9fdd1c5975655f539998b306a324af":"00000000000000000000000000000000":0

AES-192-ECB Decrypt NIST KAT #7
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_192_ECB:MBEDTLS_DECRYPT:"000000000000000000000000000000
00000000000000000":"275cfc0413d8ccb70513c3859b1d0f72":"1b077a6af4b7f98229de786d7516b639":0

AES-192-ECB
Decrypt NIST KAT #8
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_192_ECB:MBEDTLS_DECRYPT:"000000000000000000000000000000
00000000000000000":"c9b8135ff1b5adc413dfd053b21bd96d":"9c2d8842e5f48f57648205d39a239af1":0

AES-192-ECB Decrypt NIST KAT #9
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_192_ECB:MBEDTLS_DECRYPT:"000000000000000000000000000000
00000000000000000":"4a3650c3371ce2eb35e389a171427440":"bff52510095f518ecca60af4205444bb":0

AES-192-ECB Decrypt NIST KAT #10
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_192_ECB:MBEDTLS_DECRYPT:"000000000000000000000000000000
00000000000000000":"b2099795e88cc158fd75ea133d7e7fbe":"fffffffffffffffffffc00000000000":0

AES-192-ECB Decrypt NIST KAT #11
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_192_ECB:MBEDTLS_DECRYPT:"000000000000000000000000000000
00000000000000000":"a6cae46fb6fadfe7a2c302a34242817b":"fffffffffffffffffffe00000000000":0

AES-192-ECB Decrypt
NIST KAT #12
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_192_ECB:MBEDTLS_DECRYPT:"000000000000000000000000000000
00000000000000000":"026a7024d6a902e0b3ffccbaa910cc3f":"ffffffffffffffffffff00000000000":0

AES-256-ECB Encrypt NIST KAT #1
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_256_ECB:MBEDTLS_ENCRYPT:"c1cc358b449909a19436cfbb3f852ef
8bcb5ed12ac7058325f56e6099aab1a1c":"00000000000000000000000000000000":"352065272169abf9856843927d
0674fd":0

AES-256-ECB Encrypt NIST KAT #2
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_256_ECB:MBEDTLS_ENCRYPT:"984ca75f4ee8d706f46c2d98c0bf4a45f5b00d791c2dfeb191b5ed8e420fd627":"00000000000000000000000000000000":"4307456a9e67813b452e15fa8ffe398":0

AES-256-ECB Encrypt NIST KAT #3
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_256_ECB:MBEDTLS_ENCRYPT:"b43d08a447ac8609baadae4ff12918b9f68fc1653f1269222f123981ded7a92f":"00000000000000000000000000000000":"4663446607354989477a5c6f0f007ef4":0

AES-256-ECB Encrypt
NIST KAT #4
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_256_ECB:MBEDTLS_ENCRYPT:"0000000000000000000000000000000000000000000000000000000000000000":"0b24af36193ce4665f2825d7b4749c98":"a9ff75bd7cf6613d3731c77c3b6d0c04":0

AES-256-ECB Encrypt NIST KAT #5
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_256_ECB:MBEDTLS_ENCRYPT:"0000000000000000000000000000000000000000000000000000000000000000":"761c1fe41a18acf20d241650611d90f1":"623a52fcea5d443e48d9181ab32c7421":0

AES-256-ECB Encrypt NIST KAT #6
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_256_ECB:MBEDTLS_ENCRYPT:"0000000000000000000000000000000000000000000000000000000000000000":"8a560769d605868ad80d819bdba03771":"38f2c7ae10612415d27ca190d27da8b4":0

AES-256-ECB Encrypt NIST KAT #7
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_256_ECB:MBEDTLS_ENCRYPT:"0000000000000000000000000000000000000000000000000000000000000000":"ffffff8000000000000000000000000":"36aff0ef7bf3280772cf4cac80a0d2b2":0

AES-256-ECB
Encrypt NIST KAT #8
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_256_ECB:MBEDTLS_ENCRYPT:"0000000000000000000000000000000000000000000000000000000000000000":"ffffffc0000000000000000000000000":"1f8eedea0f62a1406d58cfc3ecea72cf":0

AES-256-ECB Encrypt NIST KAT #9
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_256_ECB:MBEDTLS_ENCRYPT:"0000000000000000000000000000000000

00000000000000000000000000000000":"fffffe00000000000000000000000000":"abf4154a3375a1d3e6b1d454438f95a6":0

AES-256-ECB Encrypt NIST KAT #10
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_256_ECB:MBEDTLS_ENCRYPT:"ffffffffffffffffffffffffffffffffffffff8000000000000000000000000000":"00000000000000000000000000000000":"45d089c36d5c5a4efc689e3b0de10dd5":0

AES-256-ECB Encrypt NIST KAT #11
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_256_ECB:MBEDTLS_ENCRYPT:"ffffffffffffffffffffffffffffffffffffc000000000000000000000000000":"00000000000000000000000000000000":"b4da5df4becb5462e03a0ed00d295629":0

AES-256-ECB
Encrypt NIST KAT #12
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_256_ECB:MBEDTLS_ENCRYPT:"ffffffffffffffffffffffffffffffffffffe000000000000000000000000000":"00000000000000000000000000000000":"dcf4e129136c1a4b7a0f38935cc34b2b":0

AES-256-ECB Decrypt NIST KAT #1
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_256_ECB:MBEDTLS_DECRYPT:"ffffffffffffffffffffffffffffffffffffffffffffffff00000000000000000":"edf61ae362e882ddc0167474a7a77f3a":"00000000000000000000000000000000":0

AES-256-ECB Decrypt NIST KAT #2
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_256_ECB:MBEDTLS_DECRYPT:"ffffffffffffffffffffffffffffffffffffffffffffffff80000000000000000":"6168b00ba7859e0970ecfd757efecf7c":"00000000000000000000000000000000":0

AES-256-ECB Decrypt NIST KAT #3
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_256_ECB:MBEDTLS_DECRYPT:"ffffffffffffffffffffffffffffffffffffffffffffffffc0000000000000000":"d1415447866230d28bb1ea18a4cdfd02":"00000000000000000000000000000000":0

AES-256-ECB
Decrypt NIST KAT #4
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_256_ECB:MBEDTLS_DECRYPT:"f8be9ba615c5a952cabbca24f68f8593039624d524c816acda2c9183bd917cb9":"a3944b95ca0b52043584ef02151926a8":"00000000000000000000000000000000":0

AES-256-ECB Decrypt NIST KAT #5
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_256_ECB:MBEDTLS_DECRYPT:"797f8b3d176dac5b7e34a2d539c4ef367a16f8635f6264737591c5c07bf57a3e":"a74289fe73a4c123ca189ea1e1b49ad5":"00000000000000000000000000000000":0

AES-256-ECB Decrypt NIST KAT #6

depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_256_ECB:MBEDTLS_DECRYPT:"6838d40caf927749c13f0329d331f448e202c73ef52c5f73a37ca635d4c47707":"b91d4ea4488644b56cf0812fa7fcf5fc":"00000000000000000000000000000000":0

AES-256-ECB Decrypt NIST KAT #7
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_256_ECB:MBEDTLS_DECRYPT:"00000000000000000000000000000000000000000000000000000000000000000000000000000000":"623a52fcea5d443e48d9181ab32c7421":"761c1fe41a18acf20d241650611d90f1":0

AES-256-ECB
Decrypt NIST KAT #8
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_256_ECB:MBEDTLS_DECRYPT:"00000000000000000000000000000000000000000000000000000000000000000000000000000000":"38f2c7ae10612415d27ca190d27da8b4":"8a560769d605868ad80d819bdba03771":0

AES-256-ECB Decrypt NIST KAT #9
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_256_ECB:MBEDTLS_DECRYPT:"00000000000000000000000000000000000000000000000000000000000000000000000000000000":"1bc704f1bce135ceb810341b216d7abe":"91fbef2d15a97816060bee1feaa49afe":0

AES-256-ECB Decrypt NIST KAT #10
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_256_ECB:MBEDTLS_DECRYPT:"00000000000000000000000000000000000000000000000000000000000000000000000000000000":"ddc6bf790c15760d8d9aeb6f9a75fd4e":"80000000000000000000000000000000":0

AES-256-ECB Decrypt NIST KAT #11
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_256_ECB:MBEDTLS_DECRYPT:"00000000000000000000000000000000000000000000000000000000000000000000000000000000":"0a6bdc6d4c1e6280301fd8e97ddbe601":"c0000000000000000000000000000000":0

AES-256-ECB
Decrypt NIST KAT #12
depends_on:MBEDTLS_AES_C
test_vec_ecb:MBEDTLS_CIPHER_AES_256_ECB:MBEDTLS_DECRYPT:"00000000000000000000000000000000000000000000000000000000000000000000000000000000":"9b80eefb7ebe2d2b16247aa0efc72f5d":"e0000000000000000000000000000000":0

Cipher Corner Case behaviours
depends_on:MBEDTLS_AES_C
cipher_special_behaviours:
ASN.1 Write Octet String #0 (Empty string)
mbedtls_asn1_write_octet_string:"":"0400":2:2

ASN.1 Write Octet String #1 (Large buffer)
mbedtls_asn1_write_octet_string:"AABBCC":"0403AABBCC":10:5

ASN.1 Write Octet String #2 (Buffer just fits)
mbedtls_asn1_write_octet_string:"AABBCC":"0403AABBCC":5:5

ASN.1 Write Octet String #3 (Buffer too small for tag)
mbedtls_asn1_write_octet_string:"AABBCC":"0403AABBCC":4:MBEDTLS_ERR_ASN1_BUF_TOO_SMALL

ASN.1 Write Octet String #4 (Buffer too small for len)
mbedtls_asn1_write_octet_string:"AABBCC":"0403AABBCC":3:MBEDTLS_ERR_ASN1_BUF_TOO_SMALL

ASN.1 Write Octet String #5 (Buffer too small for string)
mbedtls_asn1_write_octet_string:"AABBCC":"0403AABBCC":2:MBEDTLS_ERR_ASN1_BUF_TOO_SMALL

ASN.1 Write Octet String #6 (l = 128, large buffer)
mbedtls_asn1_write_octet_string:"000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E
0F000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E0F000102030405060708090A0
B0C0D0E0F000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E0F000102030405060
708090A0B0C0D0E0F":"048180000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E
0F000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E0F000102030405060708090A0
B0C0D0E0F000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E0F000102030405060
708090A0B0C0D0E0F":140:131

ASN.1
Write Octet String #7 (l = 128, buffer just fits)
mbedtls_asn1_write_octet_string:"000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E
0F000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E0F000102030405060708090A0
B0C0D0E0F000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E0F000102030405060
708090A0B0C0D0E0F":"048180000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E
0F000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E0F000102030405060708090A0
B0C0D0E0F000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E0F000102030405060
708090A0B0C0D0E0F":131:131

ASN.1 Write Octet String #8 (l =
128, buffer too small for tag)
mbedtls_asn1_write_octet_string:"000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E
0F000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E0F000102030405060708090A0
B0C0D0E0F000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E0F000102030405060
708090A0B0C0D0E0F":"":130:MBEDTLS_ERR_ASN1_BUF_TOO_SMALL

ASN.1 Write Octet String #9 (l = 128, buffer too small for len)
mbedtls_asn1_write_octet_string:"000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E
0F000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E0F000102030405060708090A0
B0C0D0E0F000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E0F000102030405060
708090A0B0C0D0E0F":"":129:MBEDTLS_ERR_ASN1_BUF_TOO_SMALL

ASN.1 Write Octet String #9 (l = 128, buffer too small for string)
mbedtls_asn1_write_octet_string:"000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E0F000102030405060708090A0B0C0D0E0F":"":127:MBEDTLS_ERR_ASN1_BUF_TOO_SMALL

ASN.1
Write IA5 String #0 (Empty string)
mbedtls_asn1_write_ia5_string:"":"1600":2:2

ASN.1 Write IA5 String #1 (Large buffer)
mbedtls_asn1_write_ia5_string:"ABC":"1603414243":10:5

ASN.1 Write IA5 String #2 (Buffer just fits)
mbedtls_asn1_write_ia5_string:"ABC":"1603414243":5:5

ASN.1 Write IA5 String #3 (Buffer too small for tag)
mbedtls_asn1_write_ia5_string:"ABC":"":4:MBEDTLS_ERR_ASN1_BUF_TOO_SMALL

ASN.1 Write IA5 String #4 (Buffer too small for len)
mbedtls_asn1_write_ia5_string:"ABC":"":3:MBEDTLS_ERR_ASN1_BUF_TOO_SMALL

ASN.1 Write IA5 String #5 (Buffer too small for string)
mbedtls_asn1_write_ia5_string:"ABC":"":2:MBEDTLS_ERR_ASN1_BUF_TOO_SMALL

ASN.1 Write / Read Length #0 (Len = 0, short form)
mbedtls_asn1_write_len:0:"00":1:1

ASN.1 Write / Read Length #1 (Len = 127, short form)
mbedtls_asn1_write_len:127:"7F":1:1

ASN.1 Write
/ Read Length #2 (Len = 127, buffer too small)
mbedtls_asn1_write_len:127:"7F":0:MBEDTLS_ERR_ASN1_BUF_TOO_SMALL

ASN.1 Write / Read Length #3 (Len = 128, long form)
mbedtls_asn1_write_len:128:"8180":2:2

ASN.1 Write / Read Length #4 (Len = 255, long form)
mbedtls_asn1_write_len:255:"81FF":2:2

ASN.1 Write / Read Length #5 (Len = 255, buffer too small)
mbedtls_asn1_write_len:255:"81FF":1:MBEDTLS_ERR_ASN1_BUF_TOO_SMALL

ASN.1 Write / Read Length #6 (Len = 258, byte order)
mbedtls_asn1_write_len:258:"820102":3:3

ASN.1 Write / Read Length #7 (Len = 65535, long form)

mbedtls_asn1_write_len:65535:"82FFFF":3:3

ASN.1 Write / Read Length #8 (Len = 65535, buffer too small)
mbedtls_asn1_write_len:65535:"82FFFF":2:MBEDTLS_ERR_ASN1_BUF_TOO_SMALL

ASN.1 Write / Read Length #9 (Len = 66051, byte order)
mbedtls_asn1_write_len:66051:"83010203":4:4

ASN.1 Write / Read Length #10 (Len = 16777215, long form)
mbedtls_asn1_write_len:16777215:"83FFFFFF":4:4

ASN.1 Write / Read Length #11 (Len = 16777215,
buffer too small)
mbedtls_asn1_write_len:16777215:"83FFFFFF":3:MBEDTLS_ERR_ASN1_BUF_TOO_SMALL

ASN.1 Write / Read Length #12 (Len = 16909060, byte order)
mbedtls_asn1_write_len:16909060:"8401020304":5:5

ASN.1 Write / Read Length #12 (Len = 16909060, buffer too small)
mbedtls_asn1_write_len:16909060:"8401020304":4:MBEDTLS_ERR_ASN1_BUF_TOO_SMALL
-----BEGIN EC PARAMETERS-----
BggqhkjOPQMBBw==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIKkdxegP5yN840sBDxIPpiMftZss14uLaH7zoxOqrePDoAoGCCqGSM49
AwEHoUQDQgAEe2QdevrehLH2oRsilBiVuZns5M43WmL3OJWyWijUcBUX3Nxf35jT
krFBUoPxdDfr1BPnaCojwvMEcC875uLPuQ==
-----END EC PRIVATE KEY-----
00@ *H

030 *H
0)+0*H
T|%Ozb+ij? HB`n),h+@2.a_]j?WexZHyaWQA06TH;SmivP8&qPuzI,jg^s@L]vF=E`BEK_,r0A.E0:J
1bv73b!yr/_@R`xmy2aBdwe0^i_FrvD^
VHp<{W{>4b 4b+x0; L 9'P3L>BC
?z)d `E+^cDk"G5Tvd6CPI
vk]qzUp
zu[B8%eFtTUw[ZGp40*LBU#KbDevPYA/#a0pc+
?O._{S9Dyhf >U.:@#PQ Ui\Y7Rqk%Pk=|w G;}2WgR SSCI:+.}M!11(]eNW24<f;vDD}Z25<-cw
f}E#%rSa
1SEi2`1/VP'|Ti%qx&]aLKdwc<d3:";EPF.x/c]J[/j1my M/
Rdu+8D%e?/~=FhXneul(,'zb'C2
uW~QTd*yIGI@u(1
4<~u"d^>@%' #Tgra#pqqRQ%#^H
D5CH@KUuN;
-----BEGIN CERTIFICATE-----
MIIDWzCCAhKgAwIBAgIBGDA+BgkqhkiG9w0BAQowMaANMAsGCWCGSAFlAwQCAaEa
MBgGCSqGSIb3DQEBCDALBglghkgBZQMEAgGiBAICAN4wOzELMAkGA1UEBhMCTkwx

ETAPBgNVBAoTCFBvbGFyU1NMMRkwFwYDVQQDExBQb2xhclNTTCBUZXN0IENBMB4X
DTE0MDEyMDEzNTc0NVoXDTI0MDExODEzNTc0NVowNDELMAkGA1UEBhMCTkwxETAP
BgNVBAoTCFBvbGFyU1NMMRIwEAYDVQQDEwlsb2NhbGhvc3QwgZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBAN0Rip+ZurBoyirqO2ptWZftTslU5A3uzqB9oB6q6A7C
uxNA24oSjokTJKXF9frY9ZDXyMrLxf6THa/aEiNzUnlGGrqgVyt2FjGzqK/nOJsI
i2OZOgol7kXSGFi6uZMa7dRYmmMbN/z3FAifhWVJ81kybdHg6G3eUu1mtKkL2kCV
AgMBAAGjgZIwgY8wCQYDVR0TBAIwADAdBgNVHQ4EFgQU7vPH9R8VpU1HicHTImOy
36fOvVEwYwYDVR0jBFwwWoAUtFrkpbPe0lL2udWmlQ/rPrzH/f+hP6Q9MDsxCzAJ
BgNVBAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEZMBcGA1UEAxMQUG9sYXJTU0wg
VGVzdCBDQYIBADA+BgkqhkiG9w0BAQowMaANMAsGCWCGSAFlAwQCAaEaMBgGCSqG
SIb3DQEBCDALBglghkgBZQMEAgGiBAICAN4DggEBAE7T54cyUf0ByNr34JaojFam
hV0T9QSc4wJ17sX67rxYIorXU8MynaneJzFxD9utOD3dq2TON18VswhT2McDgefl
XMwivCC0nWod8Pk638QaHxbaqC7XSq0QRBfOMXwV7knLNxI8smc9UJaco39VEcGD
yCkq4By/VCWTpvJ+1hx4zZ8WoXpFJFM5m5y9oEz4lgNv/6Wu7ILztyOk2yJiSR8r
YooC4zVeUOZuDO6At/NXZuSvmKmr+tfFrFA1AA/7yR5odQbqFVNSJ+u0x1Jv8Ra6
JXA4cXsnaDaRe+Wm0L0p+2PtQWXE5npXYIbFHAA9EOC3Ab8oaP9M/F6yQMa/2is=
-----END
 CERTIFICATE-----
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
   <Configuration>Release</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\aes\crypt_and_hash.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">
   <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">

```
  <ProjectGuid>{5DBB9FC3-6FD6-CA8D-E0FA-35F1E75EFAE7}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>crypt_and_hash</RootNamespace>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')"
 Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
```

```
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup
 Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
   <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <LinkIncremental>false</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
   <LinkIncremental>false</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <ClCompile>
     <PrecompiledHeader>
     </PrecompiledHeader>
     <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>

   <PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
     <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
     <SubSystem>Console</SubSystem>
     <GenerateDebugInformation>true</GenerateDebugInformation>
     <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
     <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
   </Link>
   <ProjectReference>
     <LinkLibraryDependencies>false</LinkLibraryDependencies>
   </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
   <ClCompile>
     <PrecompiledHeader>
     </PrecompiledHeader>
     <WarningLevel>Level3</WarningLevel>
      <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
```

```
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
```

```
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
  <Import Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
ECDSA primitive random #1
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
ecdsa_prim_random:MBEDTLS_ECP_DP_SECP192R1

ECDSA primitive random #2
depends_on:MBEDTLS_ECP_DP_SECP224R1_ENABLED
ecdsa_prim_random:MBEDTLS_ECP_DP_SECP224R1

ECDSA primitive random #3
depends_on:MBEDTLS_ECP_DP_SECP256R1_ENABLED
ecdsa_prim_random:MBEDTLS_ECP_DP_SECP256R1

ECDSA primitive random #4
depends_on:MBEDTLS_ECP_DP_SECP384R1_ENABLED
ecdsa_prim_random:MBEDTLS_ECP_DP_SECP384R1

ECDSA primitive random #5
depends_on:MBEDTLS_ECP_DP_SECP521R1_ENABLED
ecdsa_prim_random:MBEDTLS_ECP_DP_SECP521R1

ECDSA primitive rfc 4754 p256
depends_on:MBEDTLS_ECP_DP_SECP256R1_ENABLED
ecdsa_prim_test_vectors:MBEDTLS_ECP_DP_SECP256R1:"DC51D3866A15BACDE33D96F992FCA99DA7E6E
F0934E7097559C27F1614C88A7F":"2442A5CC0ECD015FA3CA31DC8E2BBC70BF42D60CBCA20085E0822C
B04235E970":"6FC98BD7E50211A4A27102FA3549DF79EBCB4BF246B80945CDDFE7D509BBFD7D":"9E56F
509196784D963D1C0A401510EE7ADA3DCC5DEE04B154BF61AF1D5A6DECE":"BA7816BF8F01CFEA41414
0DE5DAE2223B00361A396177A9CB410FF61F20015AD":"CB28E0999B9C7715FD0A80D8E47A77079716CB
BF917DD72E97566EA1C066957C":"86FA3BB4E26CAD5BF90B7F81899256CE7594BB1EA0C89212748BFF3
B3D5B0315"

ECDSA
 primitive rfc 4754 p384
depends_on:MBEDTLS_ECP_DP_SECP384R1_ENABLED
ecdsa_prim_test_vectors:MBEDTLS_ECP_DP_SECP384R1:"0BEB646634BA87735D77AE4809A0EBEA865535
DE4C1E1DCB692E84708E81A5AF62E528C38B2A81B35309668D73524D9F":"96281BF8DD5E0525CA049C04
```

8D345D3082968D10FEDF5C5ACA0C64E6465A97EA5CE10C9DFEC21797415710721F437922":"447688BA947
08EB6E2E4D59F6AB6D7EDFF9301D249FE49C33096655F5D502FAD3D383B91C5E7EDAA2B714CC99D574
3CA":"B4B74E44D71A13D568003D7489908D564C7761E229C58CBFA18950096EB7463B854D7FA992F934D
927376285E63414FA":"CB00753F45A35E8BB5A03D699AC65007272C32AB0EDED1631A8B605A43FF5BED
8086072BA1E7CC2358BAECA134C825A7":"FB017B914E29149432D8BAC29A514640B46F53DDAB2C69948
084E2930F1C8F7E08E07C9C63F2D21A07DCB56A6AF56EB3":"B263A1305E057F984D38726A1B46874109F4
17BCA112674C528262A40A629AF1CBB9F516CE0FA7D2FF630863A00E8B9F"

ECDSA primitive rfc 4754
p521
depends_on:MBEDTLS_ECP_DP_SECP521R1_ENABLED
ecdsa_prim_test_vectors:MBEDTLS_ECP_DP_SECP521R1:"0065FDA3409451DCAB0A0EAD45495112A3D813
C17BFD34BDF8C1209D7DF5849120597779060A7FF9D704ADF78B570FFAD6F062E95C7E0C5D5481C5B153
B48B375FA1":"0151518F1AF0F563517EDD5485190DF95A4BF57B5CBA4CF2A9A3F6474725A35F7AFE0A6
DDEB8BEDBCD6A197E592D40188901CECD650699C9B5E456AEA5ADD19052A8":"006F3B142EA1BFFF7E
2837AD44C9E4FF6D2D34C73184BBAD90026DD5E6E85317D9DF45CAD7803C6C20035B2F3FF63AFF4E1B
A64D1C077577DA3F4286C58F0AEAE643":"00C1C2B305419F5A41344D7E4359933D734096F556197A9B244
342B8B62F46F9373778F9DE6B6497B1EF825FF24F42F9B4A4BD7382CFC3378A540B1B7F0C1B956C2F":"D
DAF35A193617ABACC417349AE20413112E6FA4E89A97EA20A9EEEE64B55D39A2192992A274FC1A836B
A3C23A3FEEBBD454D4423643CE80E2A9AC94FA54CA49F":"0154FD3836AF92D0DCA57DD5341D3053988
534FDE8318FC6AAAAB68E2E6F4339B19F2F281A7E0B22C269D93CF8794A9278880ED7DBB8D9362CAEA
CEE544320552251":"017705A7030290D1CEB605A9A1BB03FF9CDD521E87A696EC926C8C10C8362DF49753
67101F67D1CF9BCCBF2F3D239534FA509E70AAC851AE01AAC68D62F866472660"

ECDSA
write-read random #1
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
ecdsa_write_read_random:MBEDTLS_ECP_DP_SECP192R1

ECDSA write-read random #2
depends_on:MBEDTLS_ECP_DP_SECP224R1_ENABLED
ecdsa_write_read_random:MBEDTLS_ECP_DP_SECP224R1

ECDSA write-read random #3
depends_on:MBEDTLS_ECP_DP_SECP256R1_ENABLED
ecdsa_write_read_random:MBEDTLS_ECP_DP_SECP256R1

ECDSA write-read random #4
depends_on:MBEDTLS_ECP_DP_SECP384R1_ENABLED
ecdsa_write_read_random:MBEDTLS_ECP_DP_SECP384R1

ECDSA write-read random #5
depends_on:MBEDTLS_ECP_DP_SECP521R1_ENABLED
ecdsa_write_read_random:MBEDTLS_ECP_DP_SECP521R1

ECDSA deterministic test vector rfc 6979 p192 mbedtls_sha1
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED:MBEDTLS_SHA1_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP192R1:"6FAB034934E4C0FC9AE67F5B5659A9D7D1FEFD1

87EE09FD4":MBEDTLS_MD_SHA1:"sample":"98C6BD12B23EAF5E2A2045132086BE3EB8EBD62ABF6698FF":"57A22B07DEA9530F8DE9471B1DC6624472E8E2844BC25B64"

ECDSA
deterministic test vector rfc 6979 p192 sha224
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED:MBEDTLS_SHA256_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP192R1:"6FAB034934E4C0FC9AE67F5B5659A9D7D1FEFD187EE09FD4":MBEDTLS_MD_SHA224:"sample":"A1F00DAD97AEEC91C95585F36200C65F3C01812AA60378F5":"E07EC1304C7C6C9DEBBE980B9692668F81D4DE7922A0F97A"

ECDSA deterministic test vector rfc 6979 p192 mbedtls_sha256
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED:MBEDTLS_SHA256_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP192R1:"6FAB034934E4C0FC9AE67F5B5659A9D7D1FEFD187EE09FD4":MBEDTLS_MD_SHA256:"sample":"4B0B8CE98A92866A2820E20AA6B75B56382E0F9BFD5ECB55":"CCDB006926EA9565CBADC840829D8C384E06DE1F1E381B85"

ECDSA deterministic test vector rfc 6979 p192 sha384
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED:MBEDTLS_SHA512_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP192R1:"6FAB034934E4C0FC9AE67F5B5659A9D7D1FEFD187EE09FD4":MBEDTLS_MD_SHA384:"sample":"DA63BF0B9ABCF948FBB1E9167F136145F7A20426DCC287D5":"C3AA2C960972BD7A2003A57E1C4C77F0578F8AE95E31EC5E"

ECDSA
deterministic test vector rfc 6979 p192 mbedtls_sha512
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED:MBEDTLS_SHA512_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP192R1:"6FAB034934E4C0FC9AE67F5B5659A9D7D1FEFD187EE09FD4":MBEDTLS_MD_SHA512:"sample":"4D60C5AB1996BD848343B31C00850205E2EA6922DAC2E4B8":"3F6E837448F027A1BF4B34E796E32A811CBB4050908D8F67"

ECDSA deterministic test vector rfc 6979 p192 mbedtls_sha1
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED:MBEDTLS_SHA1_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP192R1:"6FAB034934E4C0FC9AE67F5B5659A9D7D1FEFD187EE09FD4":MBEDTLS_MD_SHA1:"test":"0F2141A0EBBC44D2E1AF90A50EBCFCE5E197B3B7D4DE036D":"EB18BC9E1F3D7387500CB99CF5F7C157070A8961E38700B7"

ECDSA deterministic test vector rfc 6979 p192 sha224
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED:MBEDTLS_SHA256_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP192R1:"6FAB034934E4C0FC9AE67F5B5659A9D7D1FEFD187EE09FD4":MBEDTLS_MD_SHA224:"test":"6945A1C1D1B2206B8145548F633BB61CEF04891BAF26ED34":"B7FB7FDFC339C0B9BD61A9F5A8EAF9BE58FC5CBA2CB15293"

ECDSA
deterministic test vector rfc 6979 p192 mbedtls_sha256
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED:MBEDTLS_SHA256_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP192R1:"6FAB034934E4C0FC9AE67F5B5659A9D7D1FEFD187EE09FD4":MBEDTLS_MD_SHA256:"test":"3A718BD8B4926C3B52EE6BBE67EF79B18CB6EB62B1AD97AE":"5662E6848A4A19B1F1AE2F72ACD4B8BBE50F1EAC65D9124F"

ECDSA deterministic test vector rfc 6979 p192 sha384
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED:MBEDTLS_SHA512_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP192R1:"6FAB034934E4C0FC9AE67F5B5659A9D7D1FEFD1
87EE09FD4":MBEDTLS_MD_SHA384:"test":"B234B60B4DB75A733E19280A7A6034BD6B1EE88AF5332367"
:"7994090B2D59BB782BE57E74A44C9A1C700413F8ABEFE77A"

ECDSA deterministic test vector rfc 6979 p192 mbedtls_sha512
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED:MBEDTLS_SHA512_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP192R1:"6FAB034934E4C0FC9AE67F5B5659A9D7D1FEFD1
87EE09FD4":MBEDTLS_MD_SHA512:"test":"FE4F4AE86A58B6507946715934FE2D8FF9D95B6B098FE739":
"74CF5605C98FBA0E1EF34D4B5A1577A7DCF59457CAE52290"

ECDSA
deterministic test vector rfc 6979 p224 mbedtls_sha1
depends_on:MBEDTLS_ECP_DP_SECP224R1_ENABLED:MBEDTLS_SHA1_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP224R1:"F220266E1105BFE3083E03EC7A3A654651F45E371
67E88600BF257C1":MBEDTLS_MD_SHA1:"sample":"22226F9D40A96E19C4A301CE5B74B115303C0F3A4F
D30FC257FB57AC":"66D1CDD83E3AF75605DD6E2FEFF196D30AA7ED7A2EDF7AF475403D69"

ECDSA deterministic test vector rfc 6979 p224 sha224
depends_on:MBEDTLS_ECP_DP_SECP224R1_ENABLED:MBEDTLS_SHA256_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP224R1:"F220266E1105BFE3083E03EC7A3A654651F45E371
67E88600BF257C1":MBEDTLS_MD_SHA224:"sample":"1CDFE6662DDE1E4A1EC4CDEDF6A1F5A2FB7FBD
9145C12113E6ABFD3E":"A6694FD7718A21053F225D3F46197CA699D45006C06F871808F43EBC"

ECDSA deterministic test vector rfc 6979 p224 mbedtls_sha256
depends_on:MBEDTLS_ECP_DP_SECP224R1_ENABLED:MBEDTLS_SHA256_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP224R1:"F220266E1105BFE3083E03EC7A3A654651F45E371
67E88600BF257C1":MBEDTLS_MD_SHA256:"sample":"61AA3DA010E8E8406C656BC477A7A7189895E7E8
40CDFE8FF42307BA":"BC814050DAB5D23770879494F9E0A680DC1AF7161991BDE692B10101"

ECDSA
deterministic test vector rfc 6979 p224 sha384
depends_on:MBEDTLS_ECP_DP_SECP224R1_ENABLED:MBEDTLS_SHA512_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP224R1:"F220266E1105BFE3083E03EC7A3A654651F45E371
67E88600BF257C1":MBEDTLS_MD_SHA384:"sample":"0B115E5E36F0F9EC81F1325A5952878D745E19D7B
B3EABFABA77E953":"830F34CCDFE826CCFDC81EB4129772E20E122348A2BBD889A1B1AF1D"

ECDSA deterministic test vector rfc 6979 p224 mbedtls_sha512
depends_on:MBEDTLS_ECP_DP_SECP224R1_ENABLED:MBEDTLS_SHA512_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP224R1:"F220266E1105BFE3083E03EC7A3A654651F45E371
67E88600BF257C1":MBEDTLS_MD_SHA512:"sample":"074BD1D979D5F32BF958DDC61E4FB4872ADCAFE
B2256497CDAC30397":"A4CECA196C3D5A1FF31027B33185DC8EE43F288B21AB342E5D8EB084"

ECDSA deterministic test vector rfc 6979 p224
mbedtls_sha1
depends_on:MBEDTLS_ECP_DP_SECP224R1_ENABLED:MBEDTLS_SHA1_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP224R1:"F220266E1105BFE3083E03EC7A3A654651F45E371

67E88600BF257C1":MBEDTLS_MD_SHA1:"test":"DEAA646EC2AF2EA8AD53ED66B2E2DDAA49A12EFD8
356561451F3E21C":"95987796F6CF2062AB8135271DE56AE55366C045F6D9593F53787BD2"

ECDSA deterministic test vector rfc 6979 p224 sha224
depends_on:MBEDTLS_ECP_DP_SECP224R1_ENABLED:MBEDTLS_SHA256_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP224R1:"F220266E1105BFE3083E03EC7A3A654651F45E371
67E88600BF257C1":MBEDTLS_MD_SHA224:"test":"C441CE8E261DED634E4CF84910E4C5D1D22C5CF3B7
32BB204DBEF019":"902F42847A63BDC5F6046ADA114953120F99442D76510150F372A3F4"

ECDSA deterministic test vector rfc 6979 p224 mbedtls_sha256
depends_on:MBEDTLS_ECP_DP_SECP224R1_ENABLED:MBEDTLS_SHA256_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP224R1:"F220266E1105BFE3083E03EC7A3A654651F45E371
67E88600BF257C1":MBEDTLS_MD_SHA256:"test":"AD04DDE87B84747A243A631EA47A1BA6D1FAA0591
49AD2440DE6FBA6":"178D49B1AE90E3D8B629BE3DB5683915F4E8C99FDF6E666CF37ADCFD"

ECDSA
deterministic test vector rfc 6979 p224 sha384
depends_on:MBEDTLS_ECP_DP_SECP224R1_ENABLED:MBEDTLS_SHA512_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP224R1:"F220266E1105BFE3083E03EC7A3A654651F45E371
67E88600BF257C1":MBEDTLS_MD_SHA384:"test":"389B92682E399B26518A95506B52C03BC9379A9DADF
3391A21FB0EA4":"414A718ED3249FF6DBC5B50C27F71F01F070944DA22AB1F78F559AAB"

ECDSA deterministic test vector rfc 6979 p224 mbedtls_sha512
depends_on:MBEDTLS_ECP_DP_SECP224R1_ENABLED:MBEDTLS_SHA512_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP224R1:"F220266E1105BFE3083E03EC7A3A654651F45E371
67E88600BF257C1":MBEDTLS_MD_SHA512:"test":"049F050477C5ADD858CAC56208394B5A55BAEBBE88
7FDF765047C17C":"077EB13E7005929CEFA3CD0403C7CDCC077ADF4E44F3C41B2F60ECFF"

ECDSA deterministic test vector rfc 6979 p256 mbedtls_sha1
depends_on:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA1_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP256R1:"C9AFA9D845BA75166B5C215767B1D6934E50C3D
B36E89B127B8A622B120F6721":MBEDTLS_MD_SHA1:"sample":"61340C88C3AAEBEB4F6D667F672CA975
9A6CCAA9FA8811313039EE4A35471D32":"6D7F147DAC089441BB2E2FE8F7A3FA264B9C475098FDCF6E0
0D7C996E1B8B7EB"

ECDSA
deterministic test vector rfc 6979 p256 sha224
depends_on:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA256_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP256R1:"C9AFA9D845BA75166B5C215767B1D6934E50C3D
B36E89B127B8A622B120F6721":MBEDTLS_MD_SHA224:"sample":"53B2FFF5D1752B2C689DF257C04C40
A587FABABB3F6FC2702F1343AF7CA9AA3F":"B9AFB64FDC03DC1A131C7D2386D11E349F070AA432A4A
CC918BEA988BF75C74C"

ECDSA deterministic test vector rfc 6979 p256 mbedtls_sha256
depends_on:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA256_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP256R1:"C9AFA9D845BA75166B5C215767B1D6934E50C3D
B36E89B127B8A622B120F6721":MBEDTLS_MD_SHA256:"sample":"EFD48B2AACB6A8FD1140DD9CD45E
81D69D2C877B56AAF991C34D0EA84EAF3716":"F7CB1C942D657C41D436C7A1B6E29F65F3E900DBB9AF

F4064DC4AB2F843ACDA8"

ECDSA deterministic
test vector rfc 6979 p256 sha384
depends_on:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA512_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP256R1:"C9AFA9D845BA75166B5C215767B1D6934E50C3D
B36E89B127B8A622B120F6721":MBEDTLS_MD_SHA384:"sample":"0EAFEA039B20E9B42309FB1D89E213
057CBF973DC0CFC8F129EDDDC800EF7719":"4861F0491E6998B9455193E34E7B0D284DDD7149A74B95B9
261F13ABDE940954"

ECDSA deterministic test vector rfc 6979 p256 mbedtls_sha512
depends_on:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA512_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP256R1:"C9AFA9D845BA75166B5C215767B1D6934E50C3D
B36E89B127B8A622B120F6721":MBEDTLS_MD_SHA512:"sample":"8496A60B5E9B47C825488827E0495B0
E3FA109EC4568FD3F8D1097678EB97F00":"2362AB1ADBE2B8ADF9CB9EDAB740EA6049C028114F2460F9
6554F61FAE3302FE"

ECDSA deterministic test vector rfc 6979 p256 mbedtls_sha1
depends_on:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA1_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP256R1:"C9AFA9D845BA75166B5C215767B1D6934E50C3D
B36E89B127B8A622B120F6721":MBEDTLS_MD_SHA1:"test":"0CBCC86FD6ABD1D99E703E1EC50069EE5
C0B4BA4B9AC60E409E8EC5910D81A89":"01B9D7B73DFAA60D5651EC4591A0136F87653E0FD780C3B1B
C872FFDEAE479B1"

ECDSA
deterministic test vector rfc 6979 p256 sha224
depends_on:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA256_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP256R1:"C9AFA9D845BA75166B5C215767B1D6934E50C3D
B36E89B127B8A622B120F6721":MBEDTLS_MD_SHA224:"test":"C37EDB6F0AE79D47C3C27E962FA269BB
4F441770357E114EE511F662EC34A692":"C820053A05791E521FCAAD6042D40AEA1D6B1A540138558F47D
0719800E18F2D"

ECDSA deterministic test vector rfc 6979 p256 mbedtls_sha256
depends_on:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA256_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP256R1:"C9AFA9D845BA75166B5C215767B1D6934E50C3D
B36E89B127B8A622B120F6721":MBEDTLS_MD_SHA256:"test":"F1ABB023518351CD71D881567B1EA663E
D3EFCF6C5132B354F28D3B0B7D38367":"019F4113742A2B14BD25926B49C649155F267E60D3814B4C0CC8
4250E46F0083"

ECDSA deterministic test vector rfc 6979 p256 sha384
depends_on:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA512_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP256R1:"C9AFA9D845BA75166B5C215767B1D6934E50C3D
B36E89B127B8A622B120F6721":MBEDTLS_MD_SHA384:"test":"83910E8B48BB0C74244EBDF7F07A1C541
3D61472BD941EF3920E623FBCCEBEB6":"8DDBEC54CF8CD5874883841D712142A56A8D0F218F5003CB02
96B6B509619F2C"

ECDSA

deterministic test vector rfc 6979 p256 mbedtls_sha512
depends_on:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_SHA512_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP256R1:"C9AFA9D845BA75166B5C215767B1D6934E50C3D
B36E89B127B8A622B120F6721":MBEDTLS_MD_SHA512:"test":"461D93F31B6540894788FD206C07CFA0C
C35F46FA3C91816FFF1040AD1581A04":"39AF9F15DE0DB8D97E72719C74820D304CE5226E32DEDAE6751
9E840D1194E55"

ECDSA deterministic test vector rfc 6979 p384 mbedtls_sha1
depends_on:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA1_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP384R1:"6B9D3DAD2E1B8C1C05B19875B6659F4DE23C3B6
67BF297BA9AA47740787137D896D5724E4C70A825F872C9EA60D2EDF5":MBEDTLS_MD_SHA1:"sample":"
EC748D839243D6FBEF4FC5C4859A7DFFD7F3ABDDF72014540C16D73309834FA37B9BA002899F6FDA3A4
A9386790D4EB2":"A3BCFA947BEEF4732BF247AC17F71676CB31A847B9FF0CBC9C9ED4C1A5B3FACF26F
49CA031D4857570CCB5CA4424A443"

ECDSA
deterministic test vector rfc 6979 p384 sha224
depends_on:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA256_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP384R1:"6B9D3DAD2E1B8C1C05B19875B6659F4DE23C3B6
67BF297BA9AA47740787137D896D5724E4C70A825F872C9EA60D2EDF5":MBEDTLS_MD_SHA224:"sample
":"42356E76B55A6D9B4631C865445DBE54E056D3B3431766D0509244793C3F9366450F76EE3DE43F5A1253
33A6BE060122":"9DA0C81787064021E78DF658F2FBB0B042BF304665DB721F077A4298B095E4834C082C03
D83028EFBF93A3C23940CA8D"

ECDSA deterministic test vector rfc 6979 p384 mbedtls_sha256
depends_on:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA256_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP384R1:"6B9D3DAD2E1B8C1C05B19875B6659F4DE23C3B6
67BF297BA9AA47740787137D896D5724E4C70A825F872C9EA60D2EDF5":MBEDTLS_MD_SHA256:"sample
":"21B13D1E013C7FA1392D03C5F99AF8B30C570C6F98D4EA8E354B63A21D3DAA33BDE1E888E63355D92
FA2B3C36D8FB2CD":"F3AA443FB107745BF4BD77CB3891674632068A10CA67E3D45DB2266FA7D1FEEBE
FDC63ECCD1AC42EC0CB8668A4FA0AB0"

ECDSA
deterministic test vector rfc 6979 p384 sha384
depends_on:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA512_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP384R1:"6B9D3DAD2E1B8C1C05B19875B6659F4DE23C3B6
67BF297BA9AA47740787137D896D5724E4C70A825F872C9EA60D2EDF5":MBEDTLS_MD_SHA384:"sample
":"94EDBB92A5ECB8AAD4736E56C691916B3F88140666CE9FA73D64C4EA95AD133C81A648152E44ACF96
E36DD1E80FABE46":"99EF4AEB15F178CEA1FE40DB2603138F130E740A19624526203B6351D0A3A94FA32
9C145786E679E7B82C71A38628AC8"

ECDSA deterministic test vector rfc 6979 p384 mbedtls_sha512
depends_on:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA512_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP384R1:"6B9D3DAD2E1B8C1C05B19875B6659F4DE23C3B6
67BF297BA9AA47740787137D896D5724E4C70A825F872C9EA60D2EDF5":MBEDTLS_MD_SHA512:"sample
":"ED0959D5880AB2D869AE7F6C2915C6D60F96507F9CB3E047C0046861DA4A799CFE30F35CC900056D7C
99CD7882433709":"512C8CCEEE3890A84058CE1E22DBC2198F42323CE8ACA9135329F03C068E5112DC7C
C3EF3446DEFCEB01A45C2667FDD5"

ECDSA
deterministic test vector rfc 6979 p384 mbedtls_sha1
depends_on:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA1_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP384R1:"6B9D3DAD2E1B8C1C05B19875B6659F4DE23C3B6
67BF297BA9AA47740787137D896D5724E4C70A825F872C9EA60D2EDF5":MBEDTLS_MD_SHA1:"test":"4B
C35D3A50EF4E30576F58CD96CE6BF638025EE624004A1F7789A8B8E43D0678ACD9D29876DAF46638645F
7F404B11C7":"D5A6326C494ED3FF614703878961C0FDE7B2C278F9A65FD8C4B7186201A2991695BA1C845
41327E966FA7B50F7382282"

ECDSA deterministic test vector rfc 6979 p384 sha224
depends_on:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA256_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP384R1:"6B9D3DAD2E1B8C1C05B19875B6659F4DE23C3B6
67BF297BA9AA47740787137D896D5724E4C70A825F872C9EA60D2EDF5":MBEDTLS_MD_SHA224:"test":"
E8C9D0B6EA72A0E7837FEA1D14A1A9557F29FAA45D3E7EE888FC5BF954B5E62464A9A817C47FF78B8C1
1066B24080E72":"07041D4A7A0379AC7232FF72E6F77B6DDB8F09B16CCE0EC3286B2BD43FA8C6141C53E
A5ABEF0D8231077A04540A96B66"

ECDSA
deterministic test vector rfc 6979 p384 mbedtls_sha256
depends_on:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA256_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP384R1:"6B9D3DAD2E1B8C1C05B19875B6659F4DE23C3B6
67BF297BA9AA47740787137D896D5724E4C70A825F872C9EA60D2EDF5":MBEDTLS_MD_SHA256:"test":"6
D6DEFAC9AB64DABAFE36C6BF510352A4CC27001263638E5B16D9BB51D451559F918EEDAF2293BE5B47
5CC8F0188636B":"2D46F3BECBCC523D5F1A1256BF0C9B024D879BA9E838144C8BA6BAEB4B53B47D51A
B373F9845C0514EEFB14024787265"

ECDSA deterministic test vector rfc 6979 p384 sha384
depends_on:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA512_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP384R1:"6B9D3DAD2E1B8C1C05B19875B6659F4DE23C3B6
67BF297BA9AA47740787137D896D5724E4C70A825F872C9EA60D2EDF5":MBEDTLS_MD_SHA384:"test":"8
203B63D3C853E8D77227FB377BCF7B7B772E97892A80F36AB775D509D7A5FEB0542A7F0812998DA8F1D
D3CA3CF023DB":"DDD0760448D42D8A43AF45AF836FCE4DE8BE06B485E9B61B827C2F13173923E06A73
9F040649A667BF3B828246BAA5A5"

ECDSA
deterministic test vector rfc 6979 p384 mbedtls_sha512
depends_on:MBEDTLS_ECP_DP_SECP384R1_ENABLED:MBEDTLS_SHA512_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP384R1:"6B9D3DAD2E1B8C1C05B19875B6659F4DE23C3B6
67BF297BA9AA47740787137D896D5724E4C70A825F872C9EA60D2EDF5":MBEDTLS_MD_SHA512:"test":"
A0D5D090C9980FAF3C2CE57B7AE951D31977DD11C775D314AF55F76C676447D06FB6495CD21B4B6E340
FC236584FB277":"976984E59B4C77B0E8E4460DCA3D9F20E07B9BB1F63BEEFAF576F6B2E8B224634A209
2CD3792E0159AD9CEE37659C736"

ECDSA deterministic test vector rfc 6979 p521 mbedtls_sha1
depends_on:MBEDTLS_ECP_DP_SECP521R1_ENABLED:MBEDTLS_SHA1_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP521R1:"0FAD06DAA62BA3B25D2FB40133DA757205DE67
F5BB0018FEE8C86E1B68C7E75CAA896EB32F1F47C70855836A6D16FCC1466F6D8FBEC67DB89EC0C08B0

E996B83538":MBEDTLS_MD_SHA1:"sample":"0343B6EC45728975EA5CBA6659BBB6062A5FF89EEA58BE3C80B619F322C87910FE092F7D45BB0F8EEE01ED3F20BABEC079D202AE677B243AB40B5431D497C55D75D":"0E7B0E675A9B24413D448B8CC119D2BF7B2D2DF032741C096634D6D65D0DBE3D5694625FB9E8104D3B842C1B0E2D0B98BEA19341E8676AEF66AE4EBA3D5475D5D16"

ECDSA
deterministic test vector rfc 6979 p521 sha224
depends_on:MBEDTLS_ECP_DP_SECP521R1_ENABLED:MBEDTLS_SHA256_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP521R1:"0FAD06DAA62BA3B25D2FB40133DA757205DE67F5BB0018FEE8C86E1B68C7E75CAA896EB32F1F47C70855836A6D16FCC1466F6D8FBEC67DB89EC0C08B0E996B83538":MBEDTLS_MD_SHA224:"sample":"1776331CFCDF927D666E032E00CF776187BC9FDD8E69D0DABB4109FFE1B5E2A30715F4CC923A4A5E94D2503E9ACFED92857B7F31D7152E0F8C00C15FF3D87E2ED2E":"050CB5265417FE2320BBB5A122B8E1A32BD699089851128E360E620A30C7E17BA41A666AF126CE100E5799B153B60528D5300D08489CA9178FB610A2006C254B41F"

ECDSA deterministic test vector rfc 6979 p521 mbedtls_sha256
depends_on:MBEDTLS_ECP_DP_SECP521R1_ENABLED:MBEDTLS_SHA256_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP521R1:"0FAD06DAA62BA3B25D2FB40133DA757205DE67F5BB0018FEE8C86E1B68C7E75CAA896EB32F1F47C70855836A6D16FCC1466F6D8FBEC67DB89EC0C08B0E996B83538":MBEDTLS_MD_SHA256:"sample":"1511BB4D675114FE266FC4372B87682BAECC01D3CC62CF2303C92B3526012659D16876E25C7C1E57648F23B73564D67F61C6F14D527D54972810421E7D87589E1A7":"04A171143A83163D6DF460AAF61522695F207A58B95C0644D87E52AA1A347916E4F7A72930B1BC06DBE22CE3F58264AFD23704CBB63B29B931F7DE6C9D949A7ECFC"

ECDSA
deterministic test vector rfc 6979 p521 sha384
depends_on:MBEDTLS_ECP_DP_SECP521R1_ENABLED:MBEDTLS_SHA512_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP521R1:"0FAD06DAA62BA3B25D2FB40133DA757205DE67F5BB0018FEE8C86E1B68C7E75CAA896EB32F1F47C70855836A6D16FCC1466F6D8FBEC67DB89EC0C08B0E996B83538":MBEDTLS_MD_SHA384:"sample":"1EA842A0E17D2DE4F92C15315C63DDF72685C18195C2BB95E572B9C5136CA4B4B576AD712A52BE9730627D16054BA40CC0B8D3FF035B12AE75168397F5D50C67451":"1F21A3CEE066E1961025FB048BD5FE2B7924D0CD797BABE0A83B66F1E35EEAF5FDE143FA85DC394A7DEE766523393784484BDF3E00114A1C857CDE1AA203DB65D61"

ECDSA
deterministic test vector rfc 6979 p521 mbedtls_sha512
depends_on:MBEDTLS_ECP_DP_SECP521R1_ENABLED:MBEDTLS_SHA512_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP521R1:"0FAD06DAA62BA3B25D2FB40133DA757205DE67F5BB0018FEE8C86E1B68C7E75CAA896EB32F1F47C70855836A6D16FCC1466F6D8FBEC67DB89EC0C08B0E996B83538":MBEDTLS_MD_SHA512:"sample":"0C328FAFCBD79DD77850370C46325D987CB525569FB63C5D3BC53950E6D4C5F174E25A1EE9017B5D450606ADD152B534931D7D4E8455CC91F9B15BF05EC36E377FA":"0617CCE7CF5064806C467F678D3B4080D6F1CC50AF26CA209417308281B68AF282623EAA63E5B5C0723D8B8C37FF0777B1A20F8CCB1DCCC43997F1EE0E44DA4A67A"

ECDSA deterministic test vector rfc 6979 p521 mbedtls_sha1
depends_on:MBEDTLS_ECP_DP_SECP521R1_ENABLED:MBEDTLS_SHA1_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP521R1:"0FAD06DAA62BA3B25D2FB40133DA757205DE67F5BB0018FEE8C86E1B68C7E75CAA896EB32F1F47C70855836A6D16FCC1466F6D8FBEC67DB89EC0C08B0

E996B83538":MBEDTLS_MD_SHA1:"test":"13BAD9F29ABE20DE37EBEB823C252CA0F63361284015A3BF4
30A46AAA80B87B0693F0694BD88AFE4E661FC33B094CD3B7963BED5A727ED8BD6A3A202ABE009D0367
":"1E9BB81FF7944CA409AD138DBBEE228E1AFCC0C890FC78EC8604639CB0DBDC90F717A99EAD9D272
855D00162EE9527567DD6A92CBD629805C0445282BBC916797FF"

ECDSA
deterministic test vector rfc 6979 p521 sha224
depends_on:MBEDTLS_ECP_DP_SECP521R1_ENABLED:MBEDTLS_SHA256_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP521R1:"0FAD06DAA62BA3B25D2FB40133DA757205DE67
F5BB0018FEE8C86E1B68C7E75CAA896EB32F1F47C70855836A6D16FCC1466F6D8FBEC67DB89EC0C08B0
E996B83538":MBEDTLS_MD_SHA224:"test":"1C7ED902E123E6815546065A2C4AF977B22AA8EADDB68B2
C1110E7EA44D42086BFE4A34B67DDC0E17E96536E358219B23A706C6A6E16BA77B65E1C595D43CAE17F
B":"177336676304FCB343CE028B38E7B4FBA76C1C1B277DA18CAD2A8478B2A9A9F5BEC0F3BA04F35DB
3E4263569EC6AADE8C92746E4C82F8299AE1B8F1739F8FD519A4"

ECDSA deterministic test vector rfc 6979 p521 mbedtls_sha256
depends_on:MBEDTLS_ECP_DP_SECP521R1_ENABLED:MBEDTLS_SHA256_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP521R1:"0FAD06DAA62BA3B25D2FB40133DA757205DE67
F5BB0018FEE8C86E1B68C7E75CAA896EB32F1F47C70855836A6D16FCC1466F6D8FBEC67DB89EC0C08B0
E996B83538":MBEDTLS_MD_SHA256:"test":"00E871C4A14F993C6C7369501900C4BC1E9C7B0B4BA44E04
868B30B41D8071042EB28C4C250411D0CE08CD197E4188EA4876F279F90B3D8D74A3C76E6F1E4656AA8":
"0CD52DBAA33B063C3A6CD8058A1FB0A46A4754B034FCC644766CA14DA8CA5CA9FDE00E88C1AD60C
CBA759025299079D7A427EC3CC5B619BFBC828E7769BCD694E86"

ECDSA
deterministic test vector rfc 6979 p521 sha384
depends_on:MBEDTLS_ECP_DP_SECP521R1_ENABLED:MBEDTLS_SHA512_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP521R1:"0FAD06DAA62BA3B25D2FB40133DA757205DE67
F5BB0018FEE8C86E1B68C7E75CAA896EB32F1F47C70855836A6D16FCC1466F6D8FBEC67DB89EC0C08B0
E996B83538":MBEDTLS_MD_SHA384:"test":"14BEE21A18B6D8B3C93FAB08D43E739707953244FDBE924F
A926D76669E7AC8C89DF62ED8975C2D8397A65A49DCC09F6B0AC62272741924D479354D74FF6075578C":
"133330865C067A0EAF72362A65E2D7BC4E461E8C8995C3B6226A21BD1AA78F0ED94FE536A0DCA35534F
0CD1510C41525D163FE9D74D134881E35141ED5E8E95B979"

ECDSA deterministic
test vector rfc 6979 p521 mbedtls_sha512
depends_on:MBEDTLS_ECP_DP_SECP521R1_ENABLED:MBEDTLS_SHA512_C
ecdsa_det_test_vectors:MBEDTLS_ECP_DP_SECP521R1:"0FAD06DAA62BA3B25D2FB40133DA757205DE67
F5BB0018FEE8C86E1B68C7E75CAA896EB32F1F47C70855836A6D16FCC1466F6D8FBEC67DB89EC0C08B0
E996B83538":MBEDTLS_MD_SHA512:"test":"13E99020ABF5CEE7525D16B69B229652AB6BDF2AFFCAEF3
8773B4B7D08725F10CDB93482FDCC54EDCEE91ECA4166B2A7C6265EF0CE2BD7051B7CEF945BABD47E
E6D":"1FBD0013C674AA79CB39849527916CE301C66EA7CE8B80682786AD60F98F7E78A19CA69EFF5C574
00E3B3A0AD66CE0978214D13BAF4E9AC60752F7B155E2DE4DCE3"
-----BEGIN CERTIFICATE REQUEST-----
MIIBzTCCAQYCAQAwNDELMAkGA1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NMMRIw
EAYDVQQDEwlsb2NhbGhvc3QwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAN0R
ip+ZurBoyirqO2ptWZftTslU5A3uzqB9oB6q6A7CuxNA24oSjokTJKXF9frY9ZDX
yMrLxf6THa/aEiNzUnlGGrqgVyt2FjGzqK/nOJsIi2OZOgol7kXSGFi6uZMa7dRY

```
mmMbN/z3FAifhWVJ81kybdHg6G3eUu1mtKkL2kCVAgMBAAGgKTAnBgkqhkiG9w0B
CQ4xGjAYMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgXgMD0GCSqGSIb3DQEBCjAwoA0w
CwYJYIZIAWUDBAIBoRowGAYJKoZIhvcNAQEIMAsGCWCGSAFlAwQCAaIDAgFeA4GB
ACUaCTidvzWVJNKmRrriufThGUfw5Xgdsc3Ga8Cx+vRf+bPZmR3NVkc0Zq9uc0+8
d1WXaLzbmge6IbcvTPWCLNDAWI9UzoQ6WS9myM3eDEGdruClYwb5BVLx3MvhvooK
L/H6snE1dHNPXyCNVFTJIll3bRlVMRsfZpDhmz8/ImJ4
-----END CERTIFICATE REQUEST-----
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
   <Configuration>Release</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\ssl\ssl_client1.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">

   <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid>{487A2F80-3CA3-678D-88D5-82194872CF08}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>ssl_client1</RootNamespace>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
```

```
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
 />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
```

```
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
   <PrecompiledHeader>
   </PrecompiledHeader>
   <WarningLevel>Level3</WarningLevel>
   <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
    <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
   <SubSystem>Console</SubSystem>
   <GenerateDebugInformation>true</GenerateDebugInformation>
   <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
   <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
   <PrecompiledHeader>
   </PrecompiledHeader>
   <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
 <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
   <SubSystem>Console</SubSystem>
   <GenerateDebugInformation>true</GenerateDebugInformation>
   <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
```

```
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
  </Link>
 </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
 <Import
 Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
```

</ImportGroup>
</Project>
-----BEGIN CERTIFICATE-----
MIIDhTCCAm2gAwIBAgIBBDANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UECgwIUG9sYXJTU0wxGTAXBgNVBAMMEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTcwNTA1MTMwNzEwWhcNMjcwNTA2MTMwNzEwWjA8MQswCQYDVQQGEwJOTDERMA8G
A1UECgwIUG9sYXJTU0wxGjAYBgNVBAMMEVBvbGFyU1NMIENsaWVudCAyMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAyHTEzLn5tXnpRdkUYLB9u5Pyax6f
M60Nj4o8VmXl3ETZzGaFB9X4J7BKNdBjngpuG7fa8H6r7gwQk4ZJGDTzqCrSV/Uu
1C93KYRhTYJQj6eVSHD1bk2y1RPD0hrt5kPqQhTrdOrA7R/UV06p86jt0uDBMHEw
MjDV0/YI0FZPRo7yX/k9Z5GIMC5Cst99++UMd//sMcB4j7/Cf8qtbCHWjdmLao5v
4Jv4EFbMs44TFeY0BGbH7vk2DmqV9gmaBmf0ZXH4yqSxJeD+PIs1BGe64E92hfx/
/DZrtenNLQNiTrM9AM+vdqBpVoNq0qjU51Bx5rU2BXcFbXvI5MT9TNUhXwIDAQAB
o4GSMIGPMB0GA1UdDgQWBBRxoQBzckAvVHZeM/xSj7zx3WtGITBjBgNVHSMEXDBa
gBS0WuSls97SUva51aaVD+s+vMf9/6E/pD0wOzELMAkGA1UEBhMCTkwxETAPBgNV
BAoMCFBvbGFyU1NMMRkwFwYDVQQDDBBQb2xhclNTTCBUZXN0IENBggEAMAkGA1Ud
EwQCMAAwDQYJKoZIhvcNAQEFBQADggEBAE/yq2fOqjI0jm52TwdVsTUvZ+B2s16u
C4Qj/c89iZ7VfplpOAEV9+G6gHm/gf2O7Jgj0yXfFugQ2d+lR70cH64JFn9N1Rg9
gCo5EDBLourI8R0Kkg9zdlShBv7giwqg667Qjsu+oEWVerICOqNQGolotYSZvmtJ
7RiD8I4MXB4Qt0sSjxE897pvc4ODem10zXzvedv/q11q1mUn2L1fFc1dGIguk1fn
I/XP87FCapRobUTYrF6IvdqFaUMQ7lF3GiUIvjDPb4Wt1CyHhi/tu/SfV3fmX3rs
19UeGnvC7AdQ+OwLt3nEIlSpqVKPXHKfRKZg1WzZNgCQtNB1SrZAzFc=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIC9zCCAd+gAwIBAgIBATANBgkqhkiG9w0BAQsFADAWMRQwEgYDVQQDEwtUZXN0
IHJvb3QgMjAeFw0wMTAxMDEwMDAwMDBaFw0zMDEyMzEyMzU5NTlaMBYxFDASBgNV
BAMTC1Rlc3Qgcm9vdCAyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
hqLw+KDH8+tkX9hphnydOZFoueGTY5v8WdYI6KZXoIln9IAu4Rmb6M59uLziXurg
VKuwBqOkbUZsIY0NOA6C8FpdjZL1di8Viq669vBBs9c+x9hKpx8/VVcZfTaGgqni
h5XiivQynBQ4E2KOxEQ+VjUMDqIBHYG1VXWs4KMkAeJsqDYHtmS4XsC9TXTIri5S
9IX4mE5A9+ngSTo0/6Sjwcd27uO2IQHXDC7jkxX5OH5jFPAqsVKTYDeWlCU7bvbr
iy1H9Z9uCl+M7unbAl8BKQ8leOnno3KO3lQQAPGP2EFRT0XMuUXJnfydPbzMa9FY
ufB1I8zCBZviPvO/Of3yrwIDAQABo1AwTjAMBgNVHRMEBTADAQEBMB0GA1UdDgQW
BBSUHSH6gjrYFZnS1gDvk7BpfwTKwDAfBgNVHSMEGDAWgBSUHSH6gjrYFZnS1gDv
k7BpfwTKwDANBgkqhkiG9w0BAQsFAAOCAQEATLqZGFEBO+2IiHjkn7pBkAuktmHm
jkkuFLONwe0vlxZFaabaFqSgkoS5eZ50D0dmuUkpJRNMnGK1B/ja5RewtAdxD6us
VT8JpeWYkhxaSIHjUW95jJLMVr17it8jHawI05tD26nqDjTq3C2rM4ExpAaK/Dgv
83ZHe4IdvenkXckDMIjmSsK0GfomZmKvmnfxhg4FnQvZGI48JJUqPA2dHxRhUyr4
ohBmH5Xi5oLICd85GRi8YqD00agKL99EjGulaKNEdsQkrC4ZvY6QDV0EEnbu8b4R
GfiA42UWN2dKNSqNhBOrP9g5yTcIWXh1Dwpd1Z9vhBCwmBegPqqM5IM1dQ==
-----END
CERTIFICATE-----
Debug print msg (threshold 1, level 0)
debug_print_msg_threshold:1:0:"MyFile":999:"MyFile(0999)\: Text message, 2 == 2\n"

Debug print msg (threshold 1, level 1)
debug_print_msg_threshold:1:1:"MyFile":999:"MyFile(0999)\: Text message, 2 == 2\n"

Debug print msg (threshold 1, level 2)
debug_print_msg_threshold:1:2:"MyFile":999:""

Debug print msg (threshold 0, level 1)
debug_print_msg_threshold:0:1:"MyFile":999:""

Debug print msg (threshold 0, level 5)
debug_print_msg_threshold:0:5:"MyFile":999:""

Debug print return value #1
mbedtls_debug_print_ret:"MyFile":999:"Test return value":0:"MyFile(0999)\: Test return value() returned 0 (-0x0000)\n"

Debug print return value #2
mbedtls_debug_print_ret:"MyFile":999:"Test return value":-0x1000:"MyFile(0999)\: Test return value() returned -4096 (-0x1000)\n"

Debug print return value #3
mbedtls_debug_print_ret:"MyFile":999:"Test return value":-0xFFFF:"MyFile(0999)\: Test return value() returned -65535 (-0xffff)\n"

Debug print buffer #1
mbedtls_debug_print_buf:"MyFile":999:"Test
return value":"":"MyFile(0999)\: dumping 'Test return value' (0 bytes)\n"

Debug print buffer #2
mbedtls_debug_print_buf:"MyFile":999:"Test return value":"00":"MyFile(0999)\: dumping 'Test return value' (1 bytes)\nMyFile(0999)\: 0000\: 00   .\n"

Debug print buffer #3
mbedtls_debug_print_buf:"MyFile":999:"Test return value":"000102030405060708090A0B0C0D0E0F":"MyFile(0999)\: dumping 'Test return value' (16 bytes)\nMyFile(0999)\: 0000\: 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f ....\n"

Debug print buffer #4
mbedtls_debug_print_buf:"MyFile":999:"Test return value":"000102030405060708090A0B0C0D0E0F00":"MyFile(0999)\: dumping 'Test return value' (17 bytes)\nMyFile(0999)\: 0000\: 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f ....\nMyFile(0999)\: 0010\: 00   .\n"

Debug print buffer #5
mbedtls_debug_print_buf:"MyFile":999:"Test return value":"000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F202122232425262728292A2B2C2D2E2F30":"MyFile(0999)\: dumping 'Test return value' (49 bytes)\nMyFile(0999)\: 0000\: 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f ....\nMyFile(0999)\: 0010\: 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f ....\nMyFile(0999)\: 0020\: 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f   !"#$%&'()*+,-./\nMyFile(0999)\: 0030\: 30   0\n"

Debug print certificate #1 (RSA)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_BASE64_C:MBEDTLS_RSA_C:MBEDTLS_SHA1_C
mbedtls_debug_print_crt:"data_files/server1.crt":"MyFile":999:"PREFIX_":"MyFile(0999)\: PREFIX_
#1\:\nMyFile(0999)\: cert. version \: 3\nMyFile(0999)\: serial number \: 01\nMyFile(0999)\: issuer name \:
C=NL, O=PolarSSL, CN=PolarSSL Test CA\nMyFile(0999)\: subject name \: C=NL, O=PolarSSL,
CN=PolarSSL Server 1\nMyFile(0999)\: issued on \: 2011-02-12
14\:44\:06\nMyFile(0999)\: expires on \: 2021-02-12 14\:44\:06\nMyFile(0999)\: signed using \: RSA with
SHA1\nMyFile(0999)\: RSA key size \: 2048 bits\nMyFile(0999)\: basic constraints \:
CA=false\nMyFile(0999)\: value of 'crt->rsa.N' (2048 bits) is\:\nMyFile(0999)\: a9 02 1f 3d 40 6a d5 55 53 8b fd
36 ee 82 65 2e\nMyFile(0999)\: 15 61 5e 89 bf b8 e8 45 90 db ee 88 16 52 d3 f1\nMyFile(0999)\: 43 50 47 96 12
59 64 87 6b fd 2b e0 46 f9 73 be\nMyFile(0999)\: dd cf 92 e1 91 5b ed 66 a0 6f 89 29 79 45 80 d0\nMyFile(0999)\:
83 6a d5 41 43 77 5f 39 7c 09 04 47 82 b0 57 39\nMyFile(0999)\: 70 ed a3 ec 15 19 1e a8 33 08 47 c1 05 42 a9
fd\nMyFile(0999)\: 4c c3 b4 df dd 06 1f 4d 10 51 40 67 73 13 0f 40\nMyFile(0999)\: f8 6d 81 25 5f 0a b1 53 c6 30
7e 15 39 ac f9 5a\nMyFile(0999)\: ee 7f 92 9e a6 05 5b e7 13 97 85 b5 23 92 d9 d4\nMyFile(0999)\: 24 06 d5 09
25 89 75 07 dd a6 1a 8f 3f 09 19 be\nMyFile(0999)\: ad 65 2c 64 eb 95 9b dc fe 41 5e 17 a6 da 6c
5b\nMyFile(0999)\:
69 cc 02 ba 14 2c 16 24 9c 4a dc cd d0 f7 52 67\nMyFile(0999)\: 73 f1 2d a0 23 fd 7e f4 31 ca 2d 70 ca 89 0b
04\nMyFile(0999)\: db 2e a6 4f 70 6e 9e ce bd 58 89 e2 53 59 9e 6e\nMyFile(0999)\: 5a 92 65 e2 88 3f 0c 94 19
a3 dd e5 e8 9d 95 13\nMyFile(0999)\: ed 29 db ab 70 12 dc 5a ca 6b 17 ab 52 82 54 b1\nMyFile(0999)\: value of
'crt->rsa.E' (17 bits) is\:\nMyFile(0999)\: 01 00 01\n"

Debug print certificate #2 (EC)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_BASE64_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SE
CP384R1_ENABLED:MBEDTLS_SHA256_C
mbedtls_debug_print_crt:"data_files/test-ca2.crt":"MyFile":999:"PREFIX_":"MyFile(0999)\: PREFIX_
#1\:\nMyFile(0999)\: cert. version \: 3\nMyFile(0999)\: serial number \:
C1\:43\:E2\:7E\:62\:43\:CC\:E8\nMyFile(0999)\: issuer name \: C=NL, O=PolarSSL, CN=Polarssl Test EC
CA\nMyFile(0999)\: subject name \: C=NL, O=PolarSSL, CN=Polarssl Test EC CA\nMyFile(0999)\: issued on
\: 2013-09-24 15\:49\:48\nMyFile(0999)\: expires on \: 2023-09-22
15\:49\:48\nMyFile(0999)\: signed using \: ECDSA with SHA256\nMyFile(0999)\: EC key size \: 384
bits\nMyFile(0999)\: basic constraints \: CA=true\nMyFile(0999)\: value of 'crt->eckey.Q(X)' (384 bits)
is\:\nMyFile(0999)\: c3 da 2b 34 41 37 58 2f 87 56 fe fc 89 ba 29 43\nMyFile(0999)\: 4b 4e e0 6e c3 0e 57 53 33
39 58 d4 52 b4 91 95\nMyFile(0999)\: 39 0b 23 df 5f 17 24 62 48 fc 1a 95 29 ce 2c 2d\nMyFile(0999)\: value of
'crt->eckey.Q(Y)' (384 bits) is\:\nMyFile(0999)\: 87 c2 88 52 80 af d6 6a ab 21 dd b8 d3 1c 6e 58\nMyFile(0999)\:
b8 ca e8 b2 69 8e f3 41 ad 29 c3 b4 5f 75 a7 47\nMyFile(0999)\: 6f d5 19 29 55 69 9a 53 3b 20 b4 66 16 60 33
1e\n"

Debug print mbedtls_mpi #1
mbedtls_debug_print_mpi:16:"01020304050607":"MyFile":999:"VALUE":"MyFile(0999)\: value of 'VALUE' (49
bits) is\:\nMyFile(0999)\: 01 02 03 04 05 06 07\n"

Debug print mbedtls_mpi #2
mbedtls_debug_print_mpi:16:"00000000000007":"MyFile":999:"VALUE":"MyFile(0999)\: value of 'VALUE' (3
bits) is\:\nMyFile(0999)\:
07\n"

Debug print mbedtls_mpi #3

mbedtls_debug_print_mpi:16:"00000000000000":"MyFile":999:"VALUE":"MyFile(0999)\: value of 'VALUE' (0 bits) is\:\nMyFile(0999)\: 00\n"

Debug print mbedtls_mpi #4
mbedtls_debug_print_mpi:16:"0941379d00fed1491fe15df284dfde4a142f68aa8d412023195cee66883e6290ffe703f4ea5963bf212713cee46b107c09182b5edcd955adac418bf4918e2889af48e1099d513830cec85c26ac1e158b52620e33ba8692f893efbb2f958b4424":"MyFile":999:"VALUE":"MyFile(0999)\: value of 'VALUE' (764 bits) is\:\nMyFile(0999)\: 09 41 37 9d 00 fe d1 49 1f e1 5d f2 84 df de 4a\nMyFile(0999)\: 14 2f 68 aa 8d 41 20 23 19 5c ee 66 88 3e 62 90\nMyFile(0999)\: ff e7 03 f4 ea 59 63 bf 21 27 13 ce e4 6b 10 7c\nMyFile(0999)\: 09 18 2b 5e dc d9 55 ad ac 41 8b f4 91 8e 28 89\nMyFile(0999)\: af 48 e1 09 9d 51 38 30 ce c8 5c 26 ac 1e 15 8b\nMyFile(0999)\: 52 62 0e 33 ba 86 92 f8 93 ef bb 2f 95 8b 44 24\n"

Debug print mbedtls_mpi #5
mbedtls_debug_print_mpi:16:"0000000000000000000000000000000000000000000000000000000000000941379d00fed1491fe15df284dfde4a142f68aa8d412023195cee66883e6290ffe703f4ea5963bf212713cee46b107c09182b5edcd955adac418bf4918e2889af48e1099d513830cec85c26ac1e158b52620e33ba8692f893efbb2f958b4424":"MyFile":999:"VALUE":"MyFile(0999)\:
 value of 'VALUE' (764 bits) is\:\nMyFile(0999)\: 09 41 37 9d 00 fe d1 49 1f e1 5d f2 84 df de 4a\nMyFile(0999)\: 14 2f 68 aa 8d 41 20 23 19 5c ee 66 88 3e 62 90\nMyFile(0999)\: ff e7 03 f4 ea 59 63 bf 21 27 13 ce e4 6b 10 7c\nMyFile(0999)\: 09 18 2b 5e dc d9 55 ad ac 41 8b f4 91 8e 28 89\nMyFile(0999)\: af 48 e1 09 9d 51 38 30 ce c8 5c 26 ac 1e 15 8b\nMyFile(0999)\: 52 62 0e 33 ba 86 92 f8 93 ef bb 2f 95 8b 44 24\n"

Debug print mbedtls_mpi #6
mbedtls_debug_print_mpi:16:"0000000000000000000000000000000000000000000000000000000000000941379d00fed1491fe15df284dfde4a142f68aa8d412023195cee66883e6290ffe703f4ea5963bf212713cee46b107c09182b5edcd955adac418bf4918e2889af48e1099d513830cec85c26ac1e158b52620e33ba8692f893efbb2f958b4424":"MyFile":999:"VALUE":"MyFile(0999)\:
 value of 'VALUE' (759 bits) is\:\nMyFile(0999)\: 41 37 9d 00 fe d1 49 1f e1 5d f2 84 df de 4a 14\nMyFile(0999)\: 2f 68 aa 8d 41 20 23 19 5c ee 66 88 3e 62 90 ff\nMyFile(0999)\: e7 03 f4 ea 59 63 bf 21 27 13 ce e4 6b 10 7c 09\nMyFile(0999)\: 18 2b 5e dc d9 55 ad ac 41 8b f4 91 8e 28 89 af\nMyFile(0999)\: 48 e1 09 9d 51 38 30 ce c8 5c 26 ac 1e 15 8b 52\nMyFile(0999)\: 62 0e 33 ba 86 92 f8 93 ef bb 2f 95 8b 44 24\n"
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">

```
    <Configuration>Release</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\random\gen_entropy.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">
    <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid>{DE695064-13C3-18B0-378D-8B22672BF3F4}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>gen_entropy</RootNamespace>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
```

```
 />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
    <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
   <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <LinkIncremental>false</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
   <LinkIncremental>false</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <ClCompile>
     <PrecompiledHeader>
     </PrecompiledHeader>
     <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
      <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
     <SubSystem>Console</SubSystem>
     <GenerateDebugInformation>true</GenerateDebugInformation>
     <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
     <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
```

```
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
  </Link>
```

```
 </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
   <ClCompile>
     <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
     </PrecompiledHeader>
     <Optimization>MaxSpeed</Optimization>
     <FunctionLevelLinking>true</FunctionLevelLinking>
     <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
   <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
     <SubSystem>Console</SubSystem>
     <GenerateDebugInformation>true</GenerateDebugInformation>
     <EnableCOMDATFolding>true</EnableCOMDATFolding>
     <OptimizeReferences>true</OptimizeReferences>
     <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
     <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
   </Link>
 </ItemDefinitionGroup>
  <Import Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFCzA9BgkqhkiG9w0BBQ0wMDAbBgkqhkiG9w0BBQwwDgQIE+lx5z79hVACAggA
MBEGBSsOAwIHBAjrWP2/SiR7cwSCBMgUgnI4/ZG3jidt8TZShsbKzxQ9bt9D1URm
8FBTFMk8JRowaXZyM2fx1/vEUlvKHIwpytOYO42py0lDf2qdn8iIe+8V2GLpyGcL
ifWGbDt/ctEo2jVgWT01q2PfUEirwTPTUaDR5KBjfMjGM5V5c58fnTQztAFaXFmI
VNkiQCC6AKCbmlblEcjFGBlRGgV8sOWCW+JaR5iJNdT6PhVJzJiQrfR819fGSISj
0N0Wqpj3VA8V9BeATZAjvofBCwRABDNsDqRhjgx7ZEVz8C6pNK7Ck6ZXEjXaWc12
ZvkzjLuufZ5B7klvgLzfxEtvZbQJmrQddDXZP9ICykP6D8W87EqEgk8yoxeFioOm
0/edj7AVZ3rxbxpUUHJUiYDLNXaZTksfYhL0ZsB3cEL8VofUa1K+66N/0TismNDR
4KSIjuRausXf1WJ1oh5B18zvnl2jkzCpwISf58d7UeOny3/ZR38B71EuaXO4r21e
BrG6fi9VewuUg1DHSYLIJErVcfNnVXHuT0EzPTjr0vdTUguzDUv4/YFcpEDk5jnQ
xJshBegjbt5W5gY3GTVRlyWqGKyOska3e2u4Cf7tZtP0kyy38JHLkQQXgj6dxseT
lCIipBDJX3gU7yJHMiX/OpLcJuEMakRrpWLrB0vezX9oW0weE/dFzZeiYyo2K/DI
TIFiL6FDuLUqpcYjeB1M+wbqs0f5ndXThVYi2/j73z0dwCI1WwKZH/WOdTrjYKxi
0oiLz7pHHaPoMRymWCKTwQhYnqiOXZIpfeOFcUY4JKDzgyKdvU7XLPnbt4yxOlJD
yAzX0i+bJjYjuG45XHTS8too0GFG2h6VFvOYAQsiq1qOnxVqVUvYphZBSz7D8Vql
lHXWp954AhpfUQK4mLJq/exjUIGIZb/QxbNWNv7mTMkBQxGJ6B/1Vjkv9KC04KLe
/JMnEZD+Sw5n+5j8qS6f7YOfVJ+Hqm04M1S8cc7JD4qMufLW/RvuKyBLb3sCn0Ue
D+uiTedxoJR8nm6yI0uZ4d9RpRreca0PPt0o+DhbrDWyqH19kafN7I6SrDSbBNUO
wiGBbgN4Ur9rPbzapATA/X95y+Q3CFLe/wcMLcLHJ3tnRCUo17Fx+APmrAsyBiYd
9ulUq5WcZaw3pEDpTqN+0832UOyjIwpLyVDLU5jgW04vbW41o2SW7fCa7/QxT94p
4PEAYi2MltPYQKRO7EOh+iUOHEsc8UDb6x4i75BcKhuLwZ7nmrwzg8ZO+TWMuzYb
McJ11aZ42hN9U5H65FQzaZhAAcOqxTffQXIdARGlfvr3lTRnO/RQbxyObEqGeMHP
```

```
XlDzvIMdB6b0RG4EBfpDFUpWf3Mhx4AG3bGHPjUXXhNICCMDdI49d0lNJ3nkF0nv
JsehmIOY2U6fQBEnZhn5D0rjU+nUlHvgKQKhs9yIym/K+KVUznJW4ygwFiKXysVq
QGqfn7hbBonYqLkGL99O9JyKgz/RhEMC0dKtgu6ELYJJVWnkJGTIMkp5a8ID48qW
RmFJX+v5ryvM9ePSUbLizOUddsXycJpGsu+Am5H20cTPXkwxYtNcu49eLrGoXf7E
/mD/zDqFryMK3oUBHnBJf0k/mMnzwfgHNveXApOSbflvRx39652Wugd7CxcOrIA=
-----END
 ENCRYPTED PRIVATE KEY-----
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
   <Configuration>Release</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\pkey\pk_sign.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">

 <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid>{F2E8CA55-597F-7FDC-6456-D8650FB970A3}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>pk_sign</RootNamespace>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
```

```
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
 />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
```

```
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
   <PrecompiledHeader>
   </PrecompiledHeader>
   <WarningLevel>Level3</WarningLevel>
   <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
    <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
   <SubSystem>Console</SubSystem>
   <GenerateDebugInformation>true</GenerateDebugInformation>
   <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
   <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
   <PrecompiledHeader>
   </PrecompiledHeader>
   <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
 <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
   <SubSystem>Console</SubSystem>
   <GenerateDebugInformation>true</GenerateDebugInformation>
   <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
```

```
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
  </Link>
 </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.targets"
 />
 <ImportGroup Label="ExtensionTargets">
```

```
 </ImportGroup>
</Project>
@@
expression x, y;
statement S;
@@
 x = mbedtls_malloc(...);
 y = mbedtls_malloc(...);
 ...
* if (x == NULL || y == NULL)
   S

@@
expression x, y;
statement S;
@@
 if (
*   (x = mbedtls_malloc(...)) == NULL
   ||
*   (y = mbedtls_malloc(...)) == NULL
 )
   S
```

ECJPAKE selftest

ecjpake_selftest:

ECJPAKE round one: client, valid

read_round_one:MBEDTLS_ECJPAKE_CLIENT:"41047ea6e3a4487037a9e0dbd79262b2cc273e779930fc18409ac5361c5fe669d702e147790aeb4ce7fd6575ab0f6c7fd1c335939aa863ba37ec91b7e32bb013bb2b410409f85b3d20ebd7885ce464c08d056d6428fe4dd9287aa365f131f4360ff386d846898bc4b41583c2a5197f65d78742746c12a5ec0a4ffe2f270a750a1d8fb51620934d74eb43e54df424fd96306c0117bf131afabf90a9d33d1198d905193735144104190a07700ffa4be6ae1d79ee0f06aeb544cd5addaabedf70f8623321332c54f355f0fbfec783ed359e5d0bf7377a0fc4ea7ace473c9c112b41ccd41ac56a56124104360a1cea33fce641156458e0a4eac219e96831e6aebc88b3f3752f93a0281d1bf1fb106051db9694a8d6e862a5ef1324a3d9e27894f1ee4f7c59199965a8dd4a2091847d2d22df3ee55faa2a3fb33fd2d1e055a07a7c61ecfb8d80ec00c2c9eb12":0

ECJPAKE round one: server, valid

read_round_one:MBEDTLS_ECJPAKE_SERVER:"4104accf0106ef858fa2d919331346805a78b58bbad0b844e5c7892879146187dd2666ada781bb7f111372251a8910621f634df128ac48e381fd6ef9060731f694a441041dd0bd5d4566c9bed9ce7de701b5e82e08e84b730466018ab903c79eb982172236c0c1728ae4bf73610d34de44246ef3d9c05a2236fb66a6583d7449308babce2072fe16662992e9235c25002f11b15087b82738e03c945bf7a2995dda1e98345841047ea6e3a4487037a9e0dbd79262b2cc273e779930fc18409ac5361c5fe669d702e147790aeb4ce7fd6575ab0f6c7fd1c335939aa863ba37ec91b7e32bb013bb2b4104a49558d32ed1ebfc1816af4ff09b55fcb4ca47b2a02d1e7caf1179ea3fe1395b22b861964016fabaf72c975695d93d4df0e5197fe9f040634ed59764937787be20bc4deebbf9b8d60a335f046ca3aa941e45864c7cadef9cf75b3d8b010e443ef0":0

ECJPAKE

 round one: role mismatch

read_round_one:MBEDTLS_ECJPAKE_CLIENT:"4104accf0106ef858fa2d919331346805a78b58bbad0b844e5c78

92879146187dd2666ada781bb7f111372251a8910621f634df128ac48e381fd6ef9060731f694a441041dd0bd5d4566c
9bed9ce7de701b5e82e08e84b730466018ab903c79eb982172236c0c1728ae4bf73610d34de44246ef3d9c05a2236fb6
6a6583d7449308babce2072fe16662992e9235c25002f11b15087b82738e03c945bf7a2995dda1e98345841047ea6e3a
4487037a9e0dbd79262b2cc273e779930fc18409ac5361c5fe669d702e147790aeb4ce7fd6575ab0f6c7fd1c335939aa8
63ba37ec91b7e32bb013bb2b4104a49558d32ed1ebfc1816af4ff09b55fcb4ca47b2a02d1e7caf1179ea3fe1395b22b861
964016fabaf72c975695d93d4df0e5197fe9f040634ed59764937787be20bc4deebbf9b8d60a335f046ca3aa941e45864
c7cadef9cf75b3d8b010e443ef0":MBEDTLS_ERR_ECP_VERIFY_FAILED

ECJPAKE
round one: trailing byte
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"41047ea6e3a4487037a9e0dbd79262b2cc273e779930fc18409ac
5361c5fe669d702e147790aeb4ce7fd6575ab0f6c7fd1c335939aa863ba37ec91b7e32bb013bb2b410409f85b3d20ebd7
885ce464c08d056d6428fe4dd9287aa365f131f4360ff386d846898bc4b41583c2a5197f65d78742746c12a5ec0a4ffe2f
270a750a1d8fb51620934d74eb43e54df424fd96306c0117bf131afabf90a9d33d1198d905193735144104190a07700ff
a4be6ae1d79ee0f06aeb544cd5addaabedf70f8623321332c54f355f0fbfec783ed359e5d0bf7377a0fc4ea7ace473c9c11
2b41ccd41ac56a56124104360a1cea33fce641156458e0a4eac219e96831e6aebc88b3f3752f93a0281d1bf1fb106051d
b9694a8d6e862a5ef1324a3d9e27894f1ee4f7c59199965a8dd4a2091847d2d22df3ee55faa2a3fb33fd2d1e055a07a7c6
1ecfb8d80ec00c2c9eb1200":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE
round one: KKP1: no data
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE round one: KKP1: length of first point too small
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"00":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE round one: KKP1: length of first point too big
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"01":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE round one: KKP1: no point data
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"0104":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE round one: KKP1: first point is zero
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"0100":MBEDTLS_ERR_ECP_INVALID_KEY

ECJPAKE round one: KKP1: unknown first point format
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"41057ea6e3a4487037a9e0dbd79262b2cc273e779930fc18409ac
5361c5fe669d702e147790aeb4ce7fd6575ab0f6c7fd1c335939aa863ba37ec91b7e32bb013bb2b":MBEDTLS_ERR_
ECP_FEATURE_UNAVAILABLE

ECJPAKE round one: KKP1: nothing after first point
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"41047ea6e3a4487037a9e0dbd79262b2cc273e779930fc18409ac
5361c5fe669d702e147790aeb4ce7fd6575ab0f6c7fd1c335939aa863ba37ec91b7e32bb013bb2b":MBEDTLS_ERR_
ECP_BAD_INPUT_DATA

ECJPAKE
round one: KKP1: length of second point too small
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"41047ea6e3a4487037a9e0dbd79262b2cc273e779930fc18409ac

5361c5fe669d702e147790aeb4ce7fd6575ab0f6c7fd1c335939aa863ba37ec91b7e32bb013bb2b00":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE round one: KKP1: length of second point too big
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"41047ea6e3a4487037a9e0dbd79262b2cc273e779930fc18409ac5361c5fe669d702e147790aeb4ce7fd6575ab0f6c7fd1c335939aa863ba37ec91b7e32bb013bb2b01":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE round one: KKP1: no second point data
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"41047ea6e3a4487037a9e0dbd79262b2cc273e779930fc18409ac5361c5fe669d702e147790aeb4ce7fd6575ab0f6c7fd1c335939aa863ba37ec91b7e32bb013bb2b0104":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE round one: KKP1: unknow second point format
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"41047ea6e3a4487037a9e0dbd79262b2cc273e779930fc18409ac5361c5fe669d702e147790aeb4ce7fd6575ab0f6c7fd1c335939aa863ba37ec91b7e32bb013bb2b410509f85b3d20ebd7885ce464c08d056d6428fe4dd9287aa365f131f4360ff386d846898bc4b41583c2a5197f65d78742746c12a5ec0a4ffe2f270a750a1d8fb516":MBEDTLS_ERR_ECP_FEATURE_UNAVAILABLE

ECJPAKE
round one: KKP1: nothing after second point
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"41047ea6e3a4487037a9e0dbd79262b2cc273e779930fc18409ac5361c5fe669d702e147790aeb4ce7fd6575ab0f6c7fd1c335939aa863ba37ec91b7e32bb013bb2b410409f85b3d20ebd7885ce464c08d056d6428fe4dd9287aa365f131f4360ff386d846898bc4b41583c2a5197f65d78742746c12a5ec0a4ffe2f270a750a1d8fb516":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE round one: KKP1: zero-length r
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"41047ea6e3a4487037a9e0dbd79262b2cc273e779930fc18409ac5361c5fe669d702e147790aeb4ce7fd6575ab0f6c7fd1c335939aa863ba37ec91b7e32bb013bb2b410409f85b3d20ebd7885ce464c08d056d6428fe4dd9287aa365f131f4360ff386d846898bc4b41583c2a5197f65d78742746c12a5ec0a4ffe2f270a750a1d8fb51600":MBEDTLS_ERR_ECP_INVALID_KEY

ECJPAKE
round one: KKP1: no data for r
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"41047ea6e3a4487037a9e0dbd79262b2cc273e779930fc18409ac5361c5fe669d702e147790aeb4ce7fd6575ab0f6c7fd1c335939aa863ba37ec91b7e32bb013bb2b410409f85b3d20ebd7885ce464c08d056d6428fe4dd9287aa365f131f4360ff386d846898bc4b41583c2a5197f65d78742746c12a5ec0a4ffe2f270a750a1d8fb51601":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE round one: KKP1: corrupted r
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"41047ea6e3a4487037a9e0dbd79262b2cc273e779930fc18409ac5361c5fe669d702e147790aeb4ce7fd6575ab0f6c7fd1c335939aa863ba37ec91b7e32bb013bb2b410409f85b3d20ebd7885ce464c08d056d6428fe4dd9287aa365f131f4360ff386d846898bc4b41583c2a5197f65d78742746c12a5ec0a4ffe2f270a750a1d8fb51620934d74eb43e54df424fd96306c0117bf131afabf90a9d33d1198d90519373515":MBEDTLS_ERR_ECP_VERIFY_FAILED

ECJPAKE round one: KKP1: X not on the curve
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"41047ea6e3a4487037a9e0dbd79262b2cc273e779930fc18409ac

5361c5fe669d702e147790aeb4ce7fd6575ab0f6c7fd1c335939aa863ba37ec91b7e32bb013bb2a410409f85b3d20ebd7
885ce464c08d056d6428fe4dd9287aa365f131f4360ff386d846898bc4b41583c2a5197f65d78742746c12a5ec0a4ffe2f
270a750a1d8fb51620934d74eb43e54df424fd96306c0117bf131afabf90a9d33d1198d90519373514":MBEDTLS_ER
R_ECP_INVALID_KEY

ECJPAKE
round one: KKP2: no data
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"4104190a07700ffa4be6ae1d79ee0f06aeb544cd5addaabedf70f8
623321332c54f355f0fbfec783ed359e5d0bf7377a0fc4ea7ace473c9c112b41ccd41ac56a56124104360a1cea33fce641
156458e0a4eac219e96831e6aebc88b3f3752f93a0281d1bf1fb106051db9694a8d6e862a5ef1324a3d9e27894f1ee4f7c
59199965a8dd4a2091847d2d22df3ee55faa2a3fb33fd2d1e055a07a7c61ecfb8d80ec00c2c9eb12":MBEDTLS_ERR_
ECP_BAD_INPUT_DATA

ECJPAKE round one: KKP2: length of first point too small
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"4104190a07700ffa4be6ae1d79ee0f06aeb544cd5addaabedf70f8
623321332c54f355f0fbfec783ed359e5d0bf7377a0fc4ea7ace473c9c112b41ccd41ac56a56124104360a1cea33fce641
156458e0a4eac219e96831e6aebc88b3f3752f93a0281d1bf1fb106051db9694a8d6e862a5ef1324a3d9e27894f1ee4f7c
59199965a8dd4a2091847d2d22df3ee55faa2a3fb33fd2d1e055a07a7c61ecfb8d80ec00c2c9eb1200":MBEDTLS_ER
R_ECP_BAD_INPUT_DATA

ECJPAKE
round one: KKP2: length of first point too big
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"4104190a07700ffa4be6ae1d79ee0f06aeb544cd5addaabedf70f8
623321332c54f355f0fbfec783ed359e5d0bf7377a0fc4ea7ace473c9c112b41ccd41ac56a56124104360a1cea33fce641
156458e0a4eac219e96831e6aebc88b3f3752f93a0281d1bf1fb106051db9694a8d6e862a5ef1324a3d9e27894f1ee4f7c
59199965a8dd4a2091847d2d22df3ee55faa2a3fb33fd2d1e055a07a7c61ecfb8d80ec00c2c9eb1201":MBEDTLS_ER
R_ECP_BAD_INPUT_DATA

ECJPAKE round one: KKP2: no point data
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"4104190a07700ffa4be6ae1d79ee0f06aeb544cd5addaabedf70f8
623321332c54f355f0fbfec783ed359e5d0bf7377a0fc4ea7ace473c9c112b41ccd41ac56a56124104360a1cea33fce641
156458e0a4eac219e96831e6aebc88b3f3752f93a0281d1bf1fb106051db9694a8d6e862a5ef1324a3d9e27894f1ee4f7c
59199965a8dd4a2091847d2d22df3ee55faa2a3fb33fd2d1e055a07a7c61ecfb8d80ec00c2c9eb120104":MBEDTLS_E
RR_ECP_BAD_INPUT_DATA

ECJPAKE
round one: KKP2: first point is zero
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"4104190a07700ffa4be6ae1d79ee0f06aeb544cd5addaabedf70f8
623321332c54f355f0fbfec783ed359e5d0bf7377a0fc4ea7ace473c9c112b41ccd41ac56a56124104360a1cea33fce641
156458e0a4eac219e96831e6aebc88b3f3752f93a0281d1bf1fb106051db9694a8d6e862a5ef1324a3d9e27894f1ee4f7c
59199965a8dd4a2091847d2d22df3ee55faa2a3fb33fd2d1e055a07a7c61ecfb8d80ec00c2c9eb120100":MBEDTLS_E
RR_ECP_INVALID_KEY

ECJPAKE round one: KKP2: unknown first point format
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"4104190a07700ffa4be6ae1d79ee0f06aeb544cd5addaabedf70f8
623321332c54f355f0fbfec783ed359e5d0bf7377a0fc4ea7ace473c9c112b41ccd41ac56a56124104360a1cea33fce641
156458e0a4eac219e96831e6aebc88b3f3752f93a0281d1bf1fb106051db9694a8d6e862a5ef1324a3d9e27894f1ee4f7c
59199965a8dd4a2091847d2d22df3ee55faa2a3fb33fd2d1e055a07a7c61ecfb8d80ec00c2c9eb1241057ea6e3a448703

7a9e0dbd79262b2cc273e779930fc18409ac5361c5fe669d702e147790aeb4ce7fd6575ab0f6c7fd1c335939aa863ba37
ec91b7e32bb013bb2b":MBEDTLS_ERR_ECP_FEATURE_UNAVAILABLE

ECJPAKE
round one: KKP2: nothing after first point
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"4104190a07700ffa4be6ae1d79ee0f06aeb544cd5addaabedf70f8
623321332c54f355f0fbfec783ed359e5d0bf7377a0fc4ea7ace473c9c112b41ccd41ac56a56124104360a1cea33fce641
156458e0a4eac219e96831e6aebc88b3f3752f93a0281d1bf1fb106051db9694a8d6e862a5ef1324a3d9e27894f1ee4f7c
59199965a8dd4a2091847d2d22df3ee55faa2a3fb33fd2d1e055a07a7c61ecfb8d80ec00c2c9eb1241047ea6e3a448703
7a9e0dbd79262b2cc273e779930fc18409ac5361c5fe669d702e147790aeb4ce7fd6575ab0f6c7fd1c335939aa863ba37
ec91b7e32bb013bb2b":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE round one: KKP2: length of second point too small
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"4104190a07700ffa4be6ae1d79ee0f06aeb544cd5addaabedf70f8
623321332c54f355f0fbfec783ed359e5d0bf7377a0fc4ea7ace473c9c112b41ccd41ac56a56124104360a1cea33fce641
156458e0a4eac219e96831e6aebc88b3f3752f93a0281d1bf1fb106051db9694a8d6e862a5ef1324a3d9e27894f1ee4f7c
59199965a8dd4a2091847d2d22df3ee55faa2a3fb33fd2d1e055a07a7c61ecfb8d80ec00c2c9eb1241047ea6e3a448703
7a9e0dbd79262b2cc273e779930fc18409ac5361c5fe669d702e147790aeb4ce7fd6575ab0f6c7fd1c335939aa863ba37
ec91b7e32bb013bb2b00":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE
round one: KKP2: length of second point too big
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"4104190a07700ffa4be6ae1d79ee0f06aeb544cd5addaabedf70f8
623321332c54f355f0fbfec783ed359e5d0bf7377a0fc4ea7ace473c9c112b41ccd41ac56a56124104360a1cea33fce641
156458e0a4eac219e96831e6aebc88b3f3752f93a0281d1bf1fb106051db9694a8d6e862a5ef1324a3d9e27894f1ee4f7c
59199965a8dd4a2091847d2d22df3ee55faa2a3fb33fd2d1e055a07a7c61ecfb8d80ec00c2c9eb1241047ea6e3a448703
7a9e0dbd79262b2cc273e779930fc18409ac5361c5fe669d702e147790aeb4ce7fd6575ab0f6c7fd1c335939aa863ba37
ec91b7e32bb013bb2b01":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE round one:
KKP2: no second point data
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"4104190a07700ffa4be6ae1d79ee0f06aeb544cd5addaabedf70f8
623321332c54f355f0fbfec783ed359e5d0bf7377a0fc4ea7ace473c9c112b41ccd41ac56a56124104360a1cea33fce641
156458e0a4eac219e96831e6aebc88b3f3752f93a0281d1bf1fb106051db9694a8d6e862a5ef1324a3d9e27894f1ee4f7c
59199965a8dd4a2091847d2d22df3ee55faa2a3fb33fd2d1e055a07a7c61ecfb8d80ec00c2c9eb1241047ea6e3a448703
7a9e0dbd79262b2cc273e779930fc18409ac5361c5fe669d702e147790aeb4ce7fd6575ab0f6c7fd1c335939aa863ba37
ec91b7e32bb013bb2b0104":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE round one: KKP2: unknow second point format
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"4104190a07700ffa4be6ae1d79ee0f06aeb544cd5addaabedf70f8
623321332c54f355f0fbfec783ed359e5d0bf7377a0fc4ea7ace473c9c112b41ccd41ac56a56124104360a1cea33fce641
156458e0a4eac219e96831e6aebc88b3f3752f93a0281d1bf1fb106051db9694a8d6e862a5ef1324a3d9e27894f1ee4f7c
59199965a8dd4a2091847d2d22df3ee55faa2a3fb33fd2d1e055a07a7c61ecfb8d80ec00c2c9eb1241047ea6e3a448703
7a9e0dbd79262b2cc273e779930fc18409ac5361c5fe669d702e147790aeb4ce7fd6575ab0f6c7fd1c335939aa863ba37
ec91b7e32bb013bb2b410509f85b3d20ebd7885ce464c08d056d6428fe4dd9287aa365f131f4360ff386d846898bc4b4
1583c2a5197f65d78742746c12a5ec0a4ffe2f270a750a1d8fb516":MBEDTLS_ERR_ECP_FEATURE_UNAVAILA
BLE

ECJPAKE
round one: KKP2: nothing after second point
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"4104190a07700ffa4be6ae1d79ee0f06aeb544cd5addaabedf70f8
623321332c54f355f0fbfec783ed359e5d0bf7377a0fc4ea7ace473c9c112b41ccd41ac56a56124104360a1cea33fce641
156458e0a4eac219e96831e6aebc88b3f3752f93a0281d1bf1fb106051db9694a8d6e862a5ef1324a3d9e27894f1ee4f7c
59199965a8dd4a2091847d2d22df3ee55faa2a3fb33fd2d1e055a07a7c61ecfb8d80ec00c2c9eb1241047ea6e3a448703
7a9e0dbd79262b2cc273e779930fc18409ac5361c5fe669d702e147790aeb4ce7fd6575ab0f6c7fd1c335939aa863ba37
ec91b7e32bb013bb2b410409f85b3d20ebd7885ce464c08d056d6428fe4dd9287aa365f131f4360ff386d846898bc4b4
1583c2a5197f65d78742746c12a5ec0a4ffe2f270a750a1d8fb516":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE
round one: KKP2: zero-length r
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"4104190a07700ffa4be6ae1d79ee0f06aeb544cd5addaabedf70f8
623321332c54f355f0fbfec783ed359e5d0bf7377a0fc4ea7ace473c9c112b41ccd41ac56a56124104360a1cea33fce641
156458e0a4eac219e96831e6aebc88b3f3752f93a0281d1bf1fb106051db9694a8d6e862a5ef1324a3d9e27894f1ee4f7c
59199965a8dd4a2091847d2d22df3ee55faa2a3fb33fd2d1e055a07a7c61ecfb8d80ec00c2c9eb1241047ea6e3a448703
7a9e0dbd79262b2cc273e779930fc18409ac5361c5fe669d702e147790aeb4ce7fd6575ab0f6c7fd1c335939aa863ba37
ec91b7e32bb013bb2b410409f85b3d20ebd7885ce464c08d056d6428fe4dd9287aa365f131f4360ff386d846898bc4b4
1583c2a5197f65d78742746c12a5ec0a4ffe2f270a750a1d8fb51600":MBEDTLS_ERR_ECP_INVALID_KEY

ECJPAKE round one: KKP2: no data for r
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"4104190a07700ffa4be6ae1d79ee0f06aeb544cd5addaabedf70f8
623321332c54f355f0fbfec783ed359e5d0bf7377a0fc4ea7ace473c9c112b41ccd41ac56a56124104360a1cea33fce641
156458e0a4eac219e96831e6aebc88b3f3752f93a0281d1bf1fb106051db9694a8d6e862a5ef1324a3d9e27894f1ee4f7c
59199965a8dd4a2091847d2d22df3ee55faa2a3fb33fd2d1e055a07a7c61ecfb8d80ec00c2c9eb1241047ea6e3a448703
7a9e0dbd79262b2cc273e779930fc18409ac5361c5fe669d702e147790aeb4ce7fd6575ab0f6c7fd1c335939aa863ba37
ec91b7e32bb013bb2b410409f85b3d20ebd7885ce464c08d056d6428fe4dd9287aa365f131f4360ff386d846898bc4b4
1583c2a5197f65d78742746c12a5ec0a4ffe2f270a750a1d8fb51601":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE
round one: KKP2: corrupted r
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"4104190a07700ffa4be6ae1d79ee0f06aeb544cd5addaabedf70f8
623321332c54f355f0fbfec783ed359e5d0bf7377a0fc4ea7ace473c9c112b41ccd41ac56a56124104360a1cea33fce641
156458e0a4eac219e96831e6aebc88b3f3752f93a0281d1bf1fb106051db9694a8d6e862a5ef1324a3d9e27894f1ee4f7c
59199965a8dd4a2091847d2d22df3ee55faa2a3fb33fd2d1e055a07a7c61ecfb8d80ec00c2c9eb1241047ea6e3a448703
7a9e0dbd79262b2cc273e779930fc18409ac5361c5fe669d702e147790aeb4ce7fd6575ab0f6c7fd1c335939aa863ba37
ec91b7e32bb013bb2b410409f85b3d20ebd7885ce464c08d056d6428fe4dd9287aa365f131f4360ff386d846898bc4b4
1583c2a5197f65d78742746c12a5ec0a4ffe2f270a750a1d8fb51620934d74eb43e54df424fd96306c0117bf131afabf90
a9d33d1198d90519373515":MBEDTLS_ERR_ECP_VERIFY_FAILED

ECJPAKE
round one: KKP2: X not on the curve
read_round_one:MBEDTLS_ECJPAKE_CLIENT:"4104190a07700ffa4be6ae1d79ee0f06aeb544cd5addaabedf70f8
623321332c54f355f0fbfec783ed359e5d0bf7377a0fc4ea7ace473c9c112b41ccd41ac56a56124104360a1cea33fce641
156458e0a4eac219e96831e6aebc88b3f3752f93a0281d1bf1fb106051db9694a8d6e862a5ef1324a3d9e27894f1ee4f7c
59199965a8dd4a2091847d2d22df3ee55faa2a3fb33fd2d1e055a07a7c61ecfb8d80ec00c2c9eb1241047ea6e3a448703
7a9e0dbd79262b2cc273e779930fc18409ac5361c5fe669d702e147790aeb4ce7fd6575ab0f6c7fd1c335939aa863ba37
ec91b7e32bb013bb2a410409f85b3d20ebd7885ce464c08d056d6428fe4dd9287aa365f131f4360ff386d846898bc4b4

1583c2a5197f65d78742746c12a5ec0a4ffe2f270a750a1d8fb51620934d74eb43e54df424fd96306c0117bf131afabf90a9d33d1198d90519373514":MBEDTLS_ERR_ECP_INVALID_KEY

ECJPAKE round two client: valid
read_round_two_cli:"03001741040fb22b1d5d1123e0ef9feb9d8a2e590a1f4d7ced2c2b06586e8f2a16d4eb2fda4328a20b07d8fd667654ca18c54e32a333a0845451e926ee8804fd7af0aaa7a641045516ea3e54a0d5d8b2ce786b38d383370029a5dbe4459c9dd601b408a24ae6465c8ac905b9eb03b5d3691c139ef83f1cd4200f6c9cd4ec392218a59ed243d3c820ff724a9a70b88cb86f20b434c6865aa1cd7906dd7c9bce3525f508276f26836c":0

ECJPAKE
round two client: trailing byte
read_round_two_cli:"03001741040fb22b1d5d1123e0ef9feb9d8a2e590a1f4d7ced2c2b06586e8f2a16d4eb2fda4328a20b07d8fd667654ca18c54e32a333a0845451e926ee8804fd7af0aaa7a641045516ea3e54a0d5d8b2ce786b38d383370029a5dbe4459c9dd601b408a24ae6465c8ac905b9eb03b5d3691c139ef83f1cd4200f6c9cd4ec392218a59ed243d3c820ff724a9a70b88cb86f20b434c6865aa1cd7906dd7c9bce3525f508276f26836c00":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE round two client: no data
read_round_two_cli:"":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE round two client: ECParams too short
read_round_two_cli:"0300":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE round two
client: ECParams not named curve
read_round_two_cli:"010017":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE round two client: ECParams wrong curve
read_round_two_cli:"030016":MBEDTLS_ERR_ECP_FEATURE_UNAVAILABLE

ECJPAKE round two client: no data after ECParams
read_round_two_cli:"030017":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE round two client: length of first point too small
read_round_two_cli:"03001700":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE round two client: length of first point too big
read_round_two_cli:"03001701":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE round two client: no first point data
read_round_two_cli:"0300170104":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE round two client: first point is zero
read_round_two_cli:"0300170100":MBEDTLS_ERR_ECP_INVALID_KEY

ECJPAKE round two client: unknown first point format
read_round_two_cli:"03001741050fb22b1d5d1123e0ef9feb9d8a2e590a1f4d7ced2c2b06586e8f2a16d4eb2fda4328a20b07d8fd667654ca18c54e32a333a0845451e926ee8804fd7af0aaa7a6":MBEDTLS_ERR_ECP_FEATURE_UNAV

AILABLE

ECJPAKE
round two client: nothing after first point
read_round_two_cli:"03001741040fb22b1d5d1123e0ef9feb9d8a2e590a1f4d7ced2c2b06586e8f2a16d4eb2fda4328a20b07d8fd667654ca18c54e32a333a0845451e926ee8804fd7af0aaa7a6":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE round two client: length of second point too small
read_round_two_cli:"03001741040fb22b1d5d1123e0ef9feb9d8a2e590a1f4d7ced2c2b06586e8f2a16d4eb2fda4328a20b07d8fd667654ca18c54e32a333a0845451e926ee8804fd7af0aaa7a600":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE round two client: length of second point too big
read_round_two_cli:"03001741040fb22b1d5d1123e0ef9feb9d8a2e590a1f4d7ced2c2b06586e8f2a16d4eb2fda4328a20b07d8fd667654ca18c54e32a333a0845451e926ee8804fd7af0aaa7a601":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE round two client: no second point data
read_round_two_cli:"03001741040fb22b1d5d1123e0ef9feb9d8a2e590a1f4d7ced2c2b06586e8f2a16d4eb2fda4328a20b07d8fd667654ca18c54e32a333a0845451e926ee8804fd7af0aaa7a60104":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE
round two client: unknown second point format
read_round_two_cli:"03001741040fb22b1d5d1123e0ef9feb9d8a2e590a1f4d7ced2c2b06586e8f2a16d4eb2fda4328a20b07d8fd667654ca18c54e32a333a0845451e926ee8804fd7af0aaa7a641055516ea3e54a0d5d8b2ce786b38d383370029a5dbe4459c9dd601b408a24ae6465c8ac905b9eb03b5d3691c139ef83f1cd4200f6c9cd4ec392218a59ed243d3c8":MBEDTLS_ERR_ECP_FEATURE_UNAVAILABLE

ECJPAKE round two client: nothing after second point
read_round_two_cli:"03001741040fb22b1d5d1123e0ef9feb9d8a2e590a1f4d7ced2c2b06586e8f2a16d4eb2fda4328a20b07d8fd667654ca18c54e32a333a0845451e926ee8804fd7af0aaa7a641045516ea3e54a0d5d8b2ce786b38d383370029a5dbe4459c9dd601b408a24ae6465c8ac905b9eb03b5d3691c139ef83f1cd4200f6c9cd4ec392218a59ed243d3c8":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE round two client: zero-length r
read_round_two_cli:"03001741040fb22b1d5d1123e0ef9feb9d8a2e590a1f4d7ced2c2b06586e8f2a16d4eb2fda4328a20b07d8fd667654ca18c54e32a333a0845451e926ee8804fd7af0aaa7a641045516ea3e54a0d5d8b2ce786b38d383370029a5dbe4459c9dd601b408a24ae6465c8ac905b9eb03b5d3691c139ef83f1cd4200f6c9cd4ec392218a59ed243d3c800":MBEDTLS_ERR_ECP_INVALID_KEY

ECJPAKE
round two client: no data for r
read_round_two_cli:"03001741040fb22b1d5d1123e0ef9feb9d8a2e590a1f4d7ced2c2b06586e8f2a16d4eb2fda4328a20b07d8fd667654ca18c54e32a333a0845451e926ee8804fd7af0aaa7a641045516ea3e54a0d5d8b2ce786b38d383370029a5dbe4459c9dd601b408a24ae6465c8ac905b9eb03b5d3691c139ef83f1cd4200f6c9cd4ec392218a59ed243d3c801":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE round two client: corrupted r
read_round_two_cli:"03001741040fb22b1d5d1123e0ef9feb9d8a2e590a1f4d7ced2c2b06586e8f2a16d4eb2fda4328a20b07d8fd667654ca18c54e32a333a0845451e926ee8804fd7af0aaa7a641045516ea3e54a0d5d8b2ce786b38d383370029a5dbe4459c9dd601b408a24ae6465c8ac905b9eb03b5d3691c139ef83f1cd4200f6c9cd4ec392218a59ed243d3c820ff724a9a70b88cb86f20b434c6865aa1cd7906dd7c9bce3525f508276f26836d":MBEDTLS_ERR_ECP_VERIFY_FAILED

ECJPAKE round two client: X not on the curve
read_round_two_cli:"03001741040fb22b1d5d1123e0ef9feb9d8a2e590a1f4d7ced2c2b06586e8f2a16d4eb2fda4328a20b07d8fd667654ca18c54e32a333a0845451e926ee8804fd7af0aaa7a741045516ea3e54a0d5d8b2ce786b38d383370029a5dbe4459c9dd601b408a24ae6465c8ac905b9eb03b5d3691c139ef83f1cd4200f6c9cd4ec392218a59ed243d3c820ff724a9a70b88cb86f20b434c6865aa1cd7906dd7c9bce3525f508276f26836c":MBEDTLS_ERR_ECP_INVALID_KEY

ECJPAKE
round two server: valid
read_round_two_srv:"410469d54ee85e90ce3f1246742de507e939e81d1dc1c5cb988b58c310c9fdd9524d93720b45541c83ee8841191da7ced86e3312d43623c1d63e74989aba4affd1ee4104077e8c31e20e6bedb760c13593e69f15be85c27d68cd09ccb8c4183608917c5c3d409fac39fefee82f7292d36f0d23e055913f45a52b85dd8a2052e9e129bb4d200f011f19483535a6e89a580c9b0003baf21462ece91a82cc38dbdcae60d9c54c":0

ECJPAKE round two server: trailing byte
read_round_two_srv:"410469d54ee85e90ce3f1246742de507e939e81d1dc1c5cb988b58c310c9fdd9524d93720b45541c83ee8841191da7ced86e3312d43623c1d63e74989aba4affd1ee4104077e8c31e20e6bedb760c13593e69f15be85c27d68cd09ccb8c4183608917c5c3d409fac39fefee82f7292d36f0d23e055913f45a52b85dd8a2052e9e129bb4d200f011f19483535a6e89a580c9b0003baf21462ece91a82cc38dbdcae60d9c54c00":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE
round two server: no data
read_round_two_srv:"":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE round two server: length of forst point too small
read_round_two_srv:"00":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE round two server: length of first point too big
read_round_two_srv:"01":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE round two server: no first point data
read_round_two_srv:"0104":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE round two server: first point is zero
read_round_two_srv:"0100":MBEDTLS_ERR_ECP_INVALID_KEY

ECJPAKE round two server: unknown first point format
read_round_two_srv:"410569d54ee85e90ce3f1246742de507e939e81d1dc1c5cb988b58c310c9fdd9524d93720b45541c83ee8841191da7ced86e3312d43623c1d63e74989aba4affd1ee":MBEDTLS_ERR_ECP_FEATURE_UNAVAIL

ABLE

ECJPAKE round two server: nothing after first point
read_round_two_srv:"410469d54ee85e90ce3f1246742de507e939e81d1dc1c5cb988b58c310c9fdd9524d93720b455
41c83ee8841191da7ced86e3312d43623c1d63e74989aba4affd1ee":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE
round two server: length of second point too small
read_round_two_srv:"410469d54ee85e90ce3f1246742de507e939e81d1dc1c5cb988b58c310c9fdd9524d93720b455
41c83ee8841191da7ced86e3312d43623c1d63e74989aba4affd1ee00":MBEDTLS_ERR_ECP_BAD_INPUT_DAT
A

ECJPAKE round two server: length of second point too big
read_round_two_srv:"410469d54ee85e90ce3f1246742de507e939e81d1dc1c5cb988b58c310c9fdd9524d93720b455
41c83ee8841191da7ced86e3312d43623c1d63e74989aba4affd1ee01":MBEDTLS_ERR_ECP_BAD_INPUT_DAT
A

ECJPAKE round two server: no second point data
read_round_two_srv:"410469d54ee85e90ce3f1246742de507e939e81d1dc1c5cb988b58c310c9fdd9524d93720b455
41c83ee8841191da7ced86e3312d43623c1d63e74989aba4affd1ee0104":MBEDTLS_ERR_ECP_BAD_INPUT_DA
TA

ECJPAKE round two server: unknown second point format
read_round_two_srv:"410569d54ee85e90ce3f1246742de507e939e81d1dc1c5cb988b58c310c9fdd9524d93720b455
41c83ee8841191da7ced86e3312d43623c1d63e74989aba4affd1ee4104077e8c31e20e6bedb760c13593e69f15be85c2
7d68cd09ccb8c4183608917c5c3d409fac39fefee82f7292d36f0d23e055913f45a52b85dd8a2052e9e129bb4d":MBED
TLS_ERR_ECP_FEATURE_UNAVAILABLE

ECJPAKE
round two server: nothing after second point
read_round_two_srv:"410469d54ee85e90ce3f1246742de507e939e81d1dc1c5cb988b58c310c9fdd9524d93720b455
41c83ee8841191da7ced86e3312d43623c1d63e74989aba4affd1ee4104077e8c31e20e6bedb760c13593e69f15be85c2
7d68cd09ccb8c4183608917c5c3d409fac39fefee82f7292d36f0d23e055913f45a52b85dd8a2052e9e129bb4d":MBED
TLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE round two server: zero-length r
read_round_two_srv:"410469d54ee85e90ce3f1246742de507e939e81d1dc1c5cb988b58c310c9fdd9524d93720b455
41c83ee8841191da7ced86e3312d43623c1d63e74989aba4affd1ee4104077e8c31e20e6bedb760c13593e69f15be85c2
7d68cd09ccb8c4183608917c5c3d409fac39fefee82f7292d36f0d23e055913f45a52b85dd8a2052e9e129bb4d00":MB
EDTLS_ERR_ECP_INVALID_KEY

ECJPAKE
round two server: no data for r
read_round_two_srv:"410469d54ee85e90ce3f1246742de507e939e81d1dc1c5cb988b58c310c9fdd9524d93720b455
41c83ee8841191da7ced86e3312d43623c1d63e74989aba4affd1ee4104077e8c31e20e6bedb760c13593e69f15be85c2
7d68cd09ccb8c4183608917c5c3d409fac39fefee82f7292d36f0d23e055913f45a52b85dd8a2052e9e129bb4d20":MB
EDTLS_ERR_ECP_BAD_INPUT_DATA

ECJPAKE round two server: corrupted r
read_round_two_srv:"410469d54ee85e90ce3f1246742de507e939e81d1dc1c5cb988b58c310c9fdd9524d93720b455
41c83ee8841191da7ced86e3312d43623c1d63e74989aba4affd1ee4104077e8c31e20e6bedb760c13593e69f15be85c2
7d68cd09ccb8c4183608917c5c3d409fac39fefee82f7292d36f0d23e055913f45a52b85dd8a2052e9e129bb4d200f011f
19483535a6e89a580c9b0003baf21462ece91a82cc38dbdcae60d9c54d":MBEDTLS_ERR_ECP_VERIFY_FAILED

ECJPAKE round two server: X not on curve
read_round_two_srv:"410469d54ee85e90ce3f1246742de507e939e81d1dc1c5cb988b58c310c9fdd9524d93720b455
41c83ee8841191da7ced86e3312d43623c1d63e74989aba4affd1ef4104077e8c31e20e6bedb760c13593e69f15be85c2
7d68cd09ccb8c4183608917c5c3d409fac39fefee82f7292d36f0d23e055913f45a52b85dd8a2052e9e129bb4d200f011f
19483535a6e89a580c9b0003baf21462ece91a82cc38dbdcae60d9c54c":MBEDTLS_ERR_ECP_INVALID_KEY
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIE6jAcBgoqhkiG9w0BDAEEMA4ECJUO+jJnTjpKAgIIAASCBMi9QFFLgKGYOSDR
0zyRMc87RkrvSlyRi8BibyKvTNEDq77jTr6ZEuOF1OeZ9fvdZwJeI4GkTeKkWqTw
XDjWATXHbgTX82I3T8R2iBnv6Za9uaFDtDH5gbUYSrSNzMaoyS90hc9PTJ2+TG/Y
xUe99kSvzbhAatVQE+0TWpgH+8oACRvGelnHWofw4/CKJXJctUO8l6LdhLht1kwd
YXNX0xjxpY/eLGlsUaiDBdb0D9WFjdi4fcZ46IHspqTfBUhYbpDj8IQT1vjH6yjm
cPNPstEeyfFnirvgFuHg9LXTH0cf0mJgLzgiclgRVEOel87Lei5icEFI4hDAzWna
s3YiTijc926mD5AqQ55QXPN9v6b/uAV1QyKenoYzIWC3Y4phTTeApCyV44f9oMMD
wzcYWMZoHzEIiZj/iiCF1uOSamIjunCmpiBXTI7OGXbxXvSSJ3aU9nJHqVT88/ke
nj//EzWVYAjMdNYl0bOsWoIONl3eEEnLaUrOYOTVMxGac6yy/oIKR7GP0R26N4V2
c434y0aQpn6opT+JYa83N1RwES2/NxwrHs4pcx2WShbTjg1Cw1XMHk8nQYNnM4oJ
kXWyns/k1Bay/SXgpl2NRsoWzxCR7BavB2mRcyMz3djbOYscuT4QwpB/Wf6kr6pN
gszegRtwLmVBehwvGJwL2SEx2CDHvJNhvoD7vbNiWeTFo1wW1wF4aE7p/Ee7gSRX
z14OC8NSbuYV660ntNQ9LB+Z7NDT2d6JTjSnhQHxxLBwy3OnM2/vu0eCd/5+MGjN
C4svgFsAH9qnT1VQTzmpwGBJAbD29CVvUUeBF3+up+Mr+IQU9OWWEtUZ2Fm29gs4
j4azYJUI4+RLw75yNLVgxS5r4Cc4cKGB/P7qVqdH2CmjrEk0jxyTFT/PE3Df1cz9
F8eEprdml2ktrlQ3gCD9fw0kXBsp5vwecpQDS3r2v980vnMxb5Cm7kMTMFb4/hMY
z1yaDkarkSHQk3qFYtO5DkEUXhF6fwATyqOgJYwcy/9ynzItqgbsCIYMjpXF7Yww
FNa/GQlqIbYRCd4KT64Ahus7I00vVS3b3glcC+KlDkwCJJ0M+glzHrJs3L+PiJMi
gm+YT/5FuSqJZ/JI5QP7VMovqSLEw6y6QQHSBCOxh/CGhAL/BZ9A9afvPTRiI9OF
fyxAaf8KH1YPI3uKIuDcms0d0gJqQoDmLafdfggd6dwuLF3iQpDORgx80oPbjfl1
FEbU8M5DqiH+eOxgEvIL0AhMnPa4mv1brVdlxS3CyojnqxPfecXyEXrhEYJWJdsF
aYKR5bU1bY990aN6T3EDRblmHs25Fc328xS2ZJkHNxcJDruwi4EFpQVT+fukOz00
hOW2BEMFJLRflE+372LNIgSRVNI536YhF8r4r7O1jrw9McX3hzbJGAtcsXqyIO/k
hxC3x5ViqgZbDYgHz/CJJfP2RC8spp2RbZ/uDJu2YI8z8s9OXvcYv0EQmBAJxdt/
lyfkzEr/n8oRtDIkrq7lR3rjMUz7AbCfNJpqrEBFol9+qH8+jnmowL8LWBlh0v/A
pc3qWIulXOR1pbwXyAELo8wGhnJWL4WmY252S3i0Jn8Gf2kXewMRJsixStairjWD
1m0wWUVGSm5CO8Rfon8=
-----END
 ENCRYPTED PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIB/TCCAWagAwIBAgIJAPfGf/jpqWP5MA0GCSqGSIb3DQEBBQUAMA0xCzAJBgNV
BAYTAk5MMB4XDTE0MDEyMjEwMDQzM1oXDTI0MDEyMjEwMDQzM1owDTELMAkGA1UE
BhMCTkwwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAN0Rip+ZurBoyirqO2pt
WZftTslU5A3uzqB9oB6q6A7CuxNA24oSjokTJKXF9frY9ZDXyMrLxf6THa/aEiNz
UnlGGrqgVyt2FjGzqK/nOJsIi2OZOgol7kXSGFi6uZMa7dRYmmMbN/z3FAifhWVJ
81kybdHg6G3eUu1mtKkL2kCVAgMBAAGjZTBjMAkGA1UdEwQCMAAwCwYDVR0PBAQD

AgXgMEkGA1UdEQRCMECCHHd3dy5zaG90b2thbi1icmF1bnNjaHdlaWcuZGWCFHd3
dy5tYXNzaW1vLWFiYXRlLmV1hwTAqAEBhwTAqEWQMA0GCSqGSIb3DQEBBQUAA4GB
ABjx1ytrqCyFC5/0cjWnbLK9vsvLny2ZikDewfRxqJ5zAxGWLqHOr1SmUmu2DrvB
bkT9g5z19+iMhPnzJz1x7Q2m7WTIJTuUPK+hKZJATDLNhZ86h5Nkw8k9YzKcOrPm
EIqsy55CSgLU0ntljqSBvSb4ifrF1NnIWej2lSfN6r+3
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIIJKQIBAAKCAgEAo1Oc8nr6fMTqvowV+CpC55i5BZGFGc50Eb4RLBSRTH1e7Jep
dFjAVbBtyQRJSiY1ja0tgLQDDKZRwfEI+b4azse460InPHv7C1TN0upXlxuj6m9B
1IlP+sBaM7WBC6dVfPO+jVMIxgkFCaBCLhhdK1Fjf8HjkT/PkctWnho8NTwivc9+
nqRZjXe/eIcqm5HwjDDhu+gz+o0gVz9MfZNi1JyCrOyNZcy+cr2QeNnNVGnFq8xT
xtu6dLunhpmLFj2mm0Vjwa7Ypj5qAjpqTMtDvqbRuToyoyzajhMNcCAf7gwzIupJ
JFVdjdtgYAcQwzikwF5HoITJzzJ2qgxF7CmvGZNb7G99mLdLdhtclH3wAQKHYwEG
Jo7XKyNEuHPQgB+e0cg1SD1HqlAMuCfGGTWQ6me7Bjan3t0NzoTdDq6IpKTesbaY
+/9e2xn8DCrhBKLXQMZFDZqUoLYAkGPOEGgvlPnIIXAawouxCaNYEh5Uw871YMSP
T28rLdFr49dwYOtDg9foA8hDIW2Pd6KXbrZteesvA1nYzEOs+3AjrbT79Md2W8Bz
9bqBVNlNOESSqm4kiCJFmslm/6brNp0MSQd+o22PQ4xRtmP6UsTfU0ueiMpYc8TY
YhMbfnfFyo4m707ebcflPbBEN2dgupdQ66cvfCJB0QJt9upafY0lpdV1qUkCAwEA
AQKCAgEAgyuxzuSJrA8SYLptIoP+e7YiUqCOfy1Z9q3paLeUAhRmWilrxK9KuQcb
BOhWXCDXvdMpykXIdS5WVyZYCQtuyEeK8haNIHyKII2ZSB1A/3EJckysWB93hnFZ
gFHzNALOG64+iY34a+Pukc6NmCulGBcjjAWR2KOg9vyRsiRr2m1TkZHFpW9lJMLZ
mdkklRDeWhkgEiPpKv6QzMFfkzL9mregE3VgEjQfeFNaZlS2HWddhB5z4i+yTfIw
F1/VXqVg2y8dcP4VrV5PET8NBGPzInkj0lk1NeveE2Cl2DlUq4BMyWvUFkQhAL8B
Zd4GzmL9nimZ6Qb8dVWYC/YTahoIL3+YUCZAGIeczAo6dryheUsj1w3pSErOIY9U
dGSyq9I9XYXqcRNeyfkoNVOZ7ugqk4DvMyv64tt+NIIy9SZGcHuWo3GL0FdKiR5c
Xbn18tD+Wwrka0O1ntvzX1qkwJcpvu5+xNVbobkM4DiluoivOq+29CGANtG2Et7S
m6KCUwSElKsvpI4dNW4nWcbdj8i8gcLiKjqRu9n2BdkvAHaMhVbl9xnp9sveGLcR
iFg6mDsCQuVEH8bGPIMIav/3VUjy1wbMAA54PsqKM0aTA+DHnleXchVAhMm9eHD8
yrV8eb8/bcCbWvhDDi80kuRIaDSsYTwMWpzjz6MU9v8OuFGZZaECggEBANL44VQ7
7tok5XeJJgnRV/PGNlHKksctPMj+ye8iSDrRvHVlHHqvZ26MZJPgXwHCO/NVIWv6
hfCYlfmP/63fZ1WJqDUDxHOgjIbPtOIKTsJi3PbbODVrsycZ3y5OjpbjXKG97cKM
6RX6zbnjtGKPfbUJx+kuAOxmkFLiLJGNlLqzaJafkgWjUAV/nT6Qm2663msfZ/Md
7uDFDNOTbPS74ki5JTjlj8xmxAPcnxjNJ2ijDQ7eiCAm6JozJYy9PYixmuScFF2x
D2N6E9/JWUcYezybUgOLzbwzvJkCRJoBXj09F8cb3m6ZQ04n2peQg/0bn6HUVovF
opZJW9uZTRmFae0CggEBAMYveBnYRXyWqENf8PZ8xlqiOvJBARaIYQOPy1t4LeOv
t4ssvkSJPEG0tP2IT6ptecNN9CVRdPJn7tsgvjgPvqgymLlaw8DheFS3EK4sFd0a
SIwrYcXY8fyAFuGbbcx2JTfmxwLGYXeWG4MDkcYctUhXiObMb0YI2eXlTu4JXqJH
q1myl7pi3gux7JcFjr0ANh9mDOYXzL52WqZObaVUUNn8p/aNWpati9Z9PL2uJNxY
myZbTqWGTpZ8XlZnZYg8bHVJGoc7/seSDEnSreGQtXl6MrnsN9bDU6UhufI0iAiH
fCeELpxjBpvZi2TzYnltX+21f3oUXurXT4eYPJm6YU0CggEBAIrJUSphtvJovU/S
uGRTBEIIzekmk0JWHxu2iU84RT30hb7QwlhvFWLjFrM1MirtBRVBlpf7Gau6JUck
lLVkNw1NXotprA3Iu0lgUIU29LLp6KS4eBSkghmh6nEDGshmT6TTVhrbKebctAOq
qRsBfFfhVFKwgckCe8Uapukls4bSyWX1GVF+KwFC/0WOScIhSno8Ed0cfu38k0CI
RnAFPYpLyhHQ6rUzkZVcyIi/RUKPqOJ0QCaukewG45ffUiCffd8QUlGETjRJtdNN
GN8tWrz3DI/qo3BAtLwPguOxLLaqfv7r9Xradi1vCF0Wo82ZI32JO1n9rMSjA7vF
8LNuUc0CggEAedBPh8Mw4qVPgyoDV93VpXu1s5VU796fkqrdmblCq4Ij1L2JrWKU
0OYboQIZxW1IvEy71fw9X4mWfMWhZZ/31jZTPQqW64UqixeCfyvFvIMdOFqp3Au+
oS6x4bXBRT0RH00P4ZrB6dkvy9Vz0ktu+aokEYhylJ94HyBU5WaI7kITBi0JqZx/

Urzn6OOXmn/4xE/becoDJMZmbXYjWs16bKIpMxgrKBY/r3SG0yeorG8h3e+dZYwp
3cFP0tf2xkgteeGXFqw/q7cPKoj+K3jgsmvzpeeVYsHoNcWHH2I+gs+T9k3+wEz1
kPGkBka6rlwV7Gv0kLrYpIv27CcciHjQuQKCAQActQM3DTC3pzEwwPeYMnSXL9/s
uDqbj3MV6H8fxPIGJWfpDst7nWXhT81uKG6fYmeg5Z6nJXfP0dUF5TpW1zk6VGwn
t/ch6U7HYpseZsywdZPVIo/upgkowXSl6mfqyxzGngXuORh4zhRpcn4GTwzHG2Te
xNqMEb/i/IWnvtfvyfhEBewJcMr9Npwrg615pCiZ8y3cjvJf/gl0cGZ5LIuWBQB5
F16JxF3mm1XCukTXZO90vg3Y1JxeB+YYyF+1aQL+DgvhGZNRrGrBT/QuXQpiMCMf
VM9oZVrI7cYVNnPBEoHVcyP21NQ5AWoFTaSpMJiHZ4FBie0BGO6IkzMcG23r
-----END
RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDfTCCAmWgAwIBAgIBBDANBgkqhkiG9w0BAQsFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UECgwIUG9sYXJTU0wxGTAXBgNVBAMMEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTcwNTA5MTM1MTA1WhcNMjcwNTEwMTM1MTA1WjA0MQswCQYDVQQGEwJOTDERMA8G
A1UECgwIUG9sYXJTU0wxEjAQBgNVBAMMCWxvY2FsaG9zdDCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBAMFNo93nzR3RBNdJcriZrA545Do8Ss86ExbQWuTN
owCIp+4ea5anUrSQ7y1yej4kmvy2NKwk9XfgJmSMnLAofaHa6ozmyRyWvP7BBFKz
NtSj+uGxdtiQwWG0ZlI2oiZTqqt0Xgd9GYLbKtgfoNkNHC1JZvdbJXNG6AuKT2kM
tQCQ4dqCEGZ9rlQri2V5kaHiYcPNQEkI7mgM8YuG0ka/0LiqEQMef1aoGh5EGA8P
hYvai0Re4hjGYi/HZo36Xdh98yeJKQHFkA4/J/EwyEoO79bex8cna8cFPXrEAjya
HT4P6DSYW8tzS1KW2BGiLICIaTla0w+w3lkvEcf36hIBMJcCAwEAAaOBkjCBjzAd
BgNVHQ4EFgQUpQXoZLjc32APUBJNYKhkr02LQ5MwYwYDVR0jBFwwWoAUtFrkpbPe
0lL2udWmlQ/rPrzH/f+hP6Q9MDsxCzAJBgNVBAYTAk5MMREwDwYDVQQKDAhQb2xh
clNTTDEZMBcGA1UEAwwQUG9sYXJTU0wgVGVzdCBDQYIBADAJBgNVHRMEAjAAMA0G
CSqGSIb3DQEBCwUAA4IBAQAQf85QSjAeP+l6hirPorUL+k/3BznAh/6RXdveBO3K
uwtqK5qI59+3N+ZLXP7fr2Z5eO8qpchRgNNwT0LKglAEXGWn30PYI1GKSiqAaK0X
CUNIrxV3qKqOLbtqP1dMdiwsmiHYrN8E9UdysObedE2yDNLpTMHPJBZ+k6FowTyZ
IpUuabkxMBFxmLv+nOBDOiaCzintEcdJdY4F6p5j8jwMvVNVAXNfxAEwa0MoVRTt
/GORvq4ZEfsatVA+HRi602m+dZETTWKSODrj8AuQcG8/i1AOhk3C1WNOFKj/ZSfB
2P6EQmhLeRp4bO+3rG73T3R2yn0PZYQ7ZrjFPPKqgu+n
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIICUjCCAdegAwIBAgIJAMFD4n5iQ8zoMAoGCCqGSM49BAMCMD4xCzAJBgNVBAYT
Ak5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBF
QyBDQTAeFw0xMzA5MjQxNTQ5NDhaFw0yMzA5MjIxNTQ5NDhaMD4xCzAJBgNVBAYT
Ak5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBF
QyBDQTB2MBAGByqGSM49AgEGBSuBBAAiA2IABMPaKzRBN1gvh1b+/Im6KUNLTuBu
ww5XUzM5WNRStJGVOQsj318XJGJI/BqVKc4sLYfCiFKAr9ZqqyHduNMcbli4yuiy
aY7zQa0pw7RfdadHb9UZKVVpmlM7ILRmFmAzHqOBoDCBnTAdBgNVHQ4EFgQUnW0g
JEkBPyvLeLUZvH4kydv7NnwwbgYDVR0jBGcwZYAUnW0gJEkBPyvLeLUZvH4kydv7
NnyhQqRAMD4xCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UE
AxMTUG9sYXJzc2wgVGVzdCBFQyBDQYIJAMFD4n5iQ8zoMAwGA1UdEwQFMAMBAf8w
CgYIKoZIzj0EAwIDaQAwZgIxAMO0YnNWKJUAfXgSJtJxexn4ipg+kv4znuR50v56
t4d0PCu412mUC6Nnd7izvtE2MgIxAP1nnJQjZ8BWukszFQDG48wxCCyci9qpdSMv
uCjn8pwUOkABXK8Mss90fzCfCEOtIA==
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE REQUEST-----
MIICgTCCAWkCAQAwPDELMAkGA1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NMMRow
GAYDVQQDExFQb2xhclNTTCBTZXJ2ZXIgMTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAKkCHz1AatVVU4v9Nu6CZS4VYV6Jv7joRZDb7ogWUtPxQ1BHlhJZ
ZIdr/SvgRvlzvt3PkuGRW+1moG+JKXlFgNCDatVBQ3dfOXwJBEeCsFc5cO2j7BUZ
HqgzCEfBBUKp/UzDtN/dBh9NEFFAZ3MTD0D4bYElXwqxU8YwfhU5rPla7n+SnqYF
W+cTl4W1I5LZ1CQG1QkliXUH3aYajz8JGb6tZSxk65Wb3P5BXhem2mxbacwCuhQs
FiScStzN0PdSZ3PxLaAj/X70McotcMqJCwTbLqZPcG6ezr1YieJTWZ5uWpJl4og/
DJQZo93l6J2VE+0p26twEtxaymsXq1KCVLECAwEAAaAAMA0GCSqGSIb3DQEBDAUA
A4IBAQA/XVYxhCWWWExy+O5y/zI1121L5MPjrlLypgP+ZDU8TUq8fusryYAgVATo
njpff6RF9QTKZhouFmgwicEnE6Xuw1LZt4SWskEyISMsTemx3eiY3YSu7uqpMIIh
h5ht1qGxkFZaLG0REIlUWqVTKk9oWLOg6pv+qees00SAn031Vc2C3++ctQONUrko
fc8aAGAi9DvSuFkfjhZkp8Fr4d7buHQPmJiYxRp27K5NbVxrr0GCB3wh7ruGc8Mc
K+PNQvoz425dHK3dHzeoIWD2Ka25mbjglbW1rqAdTkZSYH2QqZTHsKCr0u5iPtSD
gF7K0AMuT2LIeSs1p82n+cLF78fz
-----END CERTIFICATE REQUEST-----
-----BEGIN CERTIFICATE-----
MIICojCCAYqgAwIBAgIBDTANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTMwODA5MDkxNzAzWhcNMjMwODA3MDkxNzAzWjA0MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxEjAQBgNVBAMTCWxvY2FsaG9zdDBJMBMGByqGSM49AgEG
CCqGSM49AwEBAzIABH0AoQyUhPABS38y67uEVs4O3RXmKKrBdUR7/L2QPB8EC2p5
fQcsej6EFasvlTdJ/6OBkjCBjzAJBgNVHRMEAjAAMB0GA1UdDgQWBBTkF2s2sgaJ
OtleQ7bgZH2Hq33eNzBjBgNVHSMEXDBagBS0WuSls97SUva51aaVD+s+vMf9/6E/
pD0wOzELMAkGA1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NMMRkwFwYDVQQDExBQ
b2xhclNTTCBUZXN0IENBggEAMA0GCSqGSIb3DQEBBQUAA4IBAQBjmSIjGKD1eH5W
4bl2MXfNIsTwc2vv/MAAhBzBEbTXd3T37+zAGPGjKncvTB+oufUVRGkoKbfoC6Jm
DYSEUuxtnUZOko/C//XlCEtK0TuS2aLEqF3gJjBJTCfthEdAhJCtmPAQDCzeKsdx
CoOtH0NQx6Xl64oDt2wYSQNWUTGLPfRpdsVEvBHhHYATQijkl2ZH8BDjsYcBicrS
qmCeN+0T1B9vrOQVEZe+fwgzVL38n8lkJZNPIbdovA9WLHwXAEzPv4la3w0qh4Tb
kSb8HtILl4I474QxrFywylyXR/p2znPleRIRgB5HtUp9tLSWkB0bwMlqQlg2EHXu
CAQ1sXmQ
-----END CERTIFICATE-----
Parse RSA Key #1 (No password when required)
depends_on:MBEDTLS_MD5_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_DES_C
pk_parse_keyfile_rsa:"data_files/test-ca.key":"NULL":MBEDTLS_ERR_PK_PASSWORD_REQUIRED

Parse RSA Key #2 (Correct password)
depends_on:MBEDTLS_MD5_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_DES_C
pk_parse_keyfile_rsa:"data_files/test-ca.key":"PolarSSLTest":0

Parse RSA Key #3 (Wrong password)
depends_on:MBEDTLS_MD5_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_DES_C
pk_parse_keyfile_rsa:"data_files/test-ca.key":"PolarSSLWRONG":MBEDTLS_ERR_PK_PASSWORD_MISMATCH

Parse RSA Key #4 (DES Encrypted)
depends_on:MBEDTLS_MD5_C:MBEDTLS_DES_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_CIPHER_MODE_CBC
pk_parse_keyfile_rsa:"data_files/keyfile.des":"testkey":0

Parse RSA Key #5 (3DES Encrypted)
depends_on:MBEDTLS_MD5_C:MBEDTLS_DES_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_CIPHER_MODE_CBC
pk_parse_keyfile_rsa:"data_files/keyfile.3des":"testkey":0

Parse RSA Key #6 (AES-128 Encrypted)
depends_on:MBEDTLS_MD5_C:MBEDTLS_AES_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_CIPHER_MODE_CBC
pk_parse_keyfile_rsa:"data_files/keyfile.aes128":"testkey":0

Parse
RSA Key #7 (AES-192 Encrypted)
depends_on:MBEDTLS_MD5_C:MBEDTLS_AES_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_CIPHER_MODE_CBC
pk_parse_keyfile_rsa:"data_files/keyfile.aes192":"testkey":0

Parse RSA Key #8 (AES-256 Encrypted)
depends_on:MBEDTLS_MD5_C:MBEDTLS_AES_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_CIPHER_MODE_CBC
pk_parse_keyfile_rsa:"data_files/keyfile.aes256":"testkey":0

Parse RSA Key #9 (PKCS#8 wrapped)
depends_on:MBEDTLS_MD5_C:MBEDTLS_PEM_PARSE_C
pk_parse_keyfile_rsa:"data_files/format_gen.key":"":0

Parse RSA Key #10 (PKCS#8 encrypted SHA1-3DES)
depends_on:MBEDTLS_DES_C:MBEDTLS_SHA1_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_PKCS12_C:MBEDTLS_CIPHER_MODE_CBC
pk_parse_keyfile_rsa:"data_files/pkcs8_pbe_sha1_3des.key":"PolarSSLTest":0

Parse RSA Key #10.1 (PKCS#8 encrypted SHA1-3DES, wrong PW)
depends_on:MBEDTLS_DES_C:MBEDTLS_SHA1_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_PKCS12_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
pk_parse_keyfile_rsa:"data_files/pkcs8_pbe_sha1_3des.key":"PolarSSLTes":MBEDTLS_ERR_PK_PASSWORD_MISMATCH

Parse
RSA Key #10.2 (PKCS#8 encrypted SHA1-3DES, no PW)
depends_on:MBEDTLS_DES_C:MBEDTLS_SHA1_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_PKCS12_C
pk_parse_keyfile_rsa:"data_files/pkcs8_pbe_sha1_3des.key":"":MBEDTLS_ERR_PK_PASSWORD_REQUIRED

Parse RSA Key #11 (PKCS#8 encrypted SHA1-3DES DER)

depends_on:MBEDTLS_DES_C:MBEDTLS_SHA1_C:MBEDTLS_PKCS12_C:MBEDTLS_CIPHER_MODE_CB
C
pk_parse_keyfile_rsa:"data_files/pkcs8_pbe_sha1_3des.der":"PolarSSLTest":0

Parse RSA Key #12 (PKCS#8 encrypted SHA1-2DES)
depends_on:MBEDTLS_DES_C:MBEDTLS_SHA1_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_PKCS12_C:MB
EDTLS_CIPHER_MODE_CBC
pk_parse_keyfile_rsa:"data_files/pkcs8_pbe_sha1_2des.key":"PolarSSLTest":0

Parse RSA Key #12.1 (PKCS#8 encrypted SHA1-2DES, wrong PW)
depends_on:MBEDTLS_DES_C:MBEDTLS_SHA1_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_PKCS12_C:MB
EDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
pk_parse_keyfile_rsa:"data_files/pkcs8_pbe_sha1_2des.key":"PolarSLTest":MBEDTLS_ERR_PK_PASSWORD_
MISMATCH

Parse
RSA Key #12.2 (PKCS#8 encrypted SHA1-2DES, no PW)
depends_on:MBEDTLS_DES_C:MBEDTLS_SHA1_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_PKCS12_C
pk_parse_keyfile_rsa:"data_files/pkcs8_pbe_sha1_2des.key":"":MBEDTLS_ERR_PK_PASSWORD_REQUIRED

Parse RSA Key #13 (PKCS#8 encrypted SHA1-RC4-128)
depends_on:MBEDTLS_ARC4_C:MBEDTLS_SHA1_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_PKCS12_C
pk_parse_keyfile_rsa:"data_files/pkcs8_pbe_sha1_rc4_128.key":"PolarSSLTest":0

Parse RSA Key #13.1 (PKCS#8 encrypted SHA1-RC4-128, wrong PW)
depends_on:MBEDTLS_ARC4_C:MBEDTLS_SHA1_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_PKCS12_C
pk_parse_keyfile_rsa:"data_files/pkcs8_pbe_sha1_rc4_128.key":"PolarSSLTe":MBEDTLS_ERR_PK_PASSWOR
D_MISMATCH

Parse RSA Key #13.2 (PKCS#8 encrypted SHA1-RC4-128, no PW)
depends_on:MBEDTLS_ARC4_C:MBEDTLS_SHA1_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_PKCS12_C
pk_parse_keyfile_rsa:"data_files/pkcs8_pbe_sha1_rc4_128.key":"":MBEDTLS_ERR_PK_PASSWORD_REQUIR
ED

Parse
RSA Key #14 (PKCS#8 encrypted v2 PBDFK2 3DES)
depends_on:MBEDTLS_DES_C:MBEDTLS_SHA1_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_PKCS5_C:MBE
DTLS_CIPHER_MODE_CBC
pk_parse_keyfile_rsa:"data_files/pkcs8_pbes2_pbkdf2_3des.key":"PolarSSLTest":0

Parse RSA Key #15 (PKCS#8 encrypted v2 PBDFK2 3DES, wrong PW)
depends_on:MBEDTLS_DES_C:MBEDTLS_SHA1_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_PKCS5_C:MBE
DTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
pk_parse_keyfile_rsa:"data_files/pkcs8_pbes2_pbkdf2_3des.key":"PolarSSLTes":MBEDTLS_ERR_PK_PASSWO
RD_MISMATCH

Parse RSA Key #16 (PKCS#8 encrypted v2 PBDFK2 3DES, no PW)
depends_on:MBEDTLS_DES_C:MBEDTLS_SHA1_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_PKCS5_C

pk_parse_keyfile_rsa:"data_files/pkcs8_pbes2_pbkdf2_3des.key":"":MBEDTLS_ERR_PK_PASSWORD_REQUIRED

Parse RSA Key #17 (PKCS#8 encrypted v2 PBDFK2 3DES DER)
depends_on:MBEDTLS_DES_C:MBEDTLS_SHA1_C:MBEDTLS_PKCS5_C:MBEDTLS_CIPHER_MODE_CBC
pk_parse_keyfile_rsa:"data_files/pkcs8_pbes2_pbkdf2_3des.der":"PolarSSLTest":0

Parse
RSA Key #18 (PKCS#8 encrypted v2 PBDFK2 3DES DER, wrong PW)
depends_on:MBEDTLS_DES_C:MBEDTLS_SHA1_C:MBEDTLS_PKCS5_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
pk_parse_keyfile_rsa:"data_files/pkcs8_pbes2_pbkdf2_3des.der":"PolarSSLTes":MBEDTLS_ERR_PK_PASSWORD_MISMATCH

Parse RSA Key #19 (PKCS#8 encrypted v2 PBDFK2 3DES DER, no PW)
depends_on:MBEDTLS_DES_C:MBEDTLS_SHA1_C:MBEDTLS_PKCS5_C
pk_parse_keyfile_rsa:"data_files/pkcs8_pbes2_pbkdf2_3des.der":"":MBEDTLS_ERR_PK_KEY_INVALID_FORMAT

Parse RSA Key #20 (PKCS#8 encrypted v2 PBDFK2 DES)
depends_on:MBEDTLS_DES_C:MBEDTLS_SHA1_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_PKCS5_C:MBEDTLS_CIPHER_MODE_CBC
pk_parse_keyfile_rsa:"data_files/pkcs8_pbes2_pbkdf2_des.key":"PolarSSLTest":0

Parse Public RSA Key #1 (PKCS#8 wrapped)
depends_on:MBEDTLS_MD5_C:MBEDTLS_PEM_PARSE_C
pk_parse_public_keyfile_rsa:"data_files/format_gen.pub":0

Parse Public EC Key #1 (RFC 5480, DER)
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP192R1_ENABLED
pk_parse_public_keyfile_ec:"data_files/ec_pub.der":0

Parse
Public EC Key #2 (RFC 5480, PEM)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP192R1_ENABLED
pk_parse_public_keyfile_ec:"data_files/ec_pub.pem":0

Parse Public EC Key #3 (RFC 5480, secp224r1)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP224R1_ENABLED
pk_parse_public_keyfile_ec:"data_files/ec_224_pub.pem":0

Parse Public EC Key #4 (RFC 5480, secp256r1)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED
pk_parse_public_keyfile_ec:"data_files/ec_256_pub.pem":0

Parse Public EC Key #5 (RFC 5480, secp384r1)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP384R1_ENABLED

pk_parse_public_keyfile_ec:"data_files/ec_384_pub.pem":0

Parse Public EC Key #6 (RFC 5480, secp521r1)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP521R1_ENABLED
pk_parse_public_keyfile_ec:"data_files/ec_521_pub.pem":0

Parse Public EC Key #7 (RFC 5480, brainpoolP256r1)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_BP256R1_ENABLED
pk_parse_public_keyfile_ec:"data_files/ec_bp256_pub.pem":0

Parse
Public EC Key #8 (RFC 5480, brainpoolP384r1)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_BP384R1_ENABLED
pk_parse_public_keyfile_ec:"data_files/ec_bp384_pub.pem":0

Parse Public EC Key #9 (RFC 5480, brainpoolP512r1)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_BP512R1_ENABLED
pk_parse_public_keyfile_ec:"data_files/ec_bp512_pub.pem":0

Parse EC Key #1 (SEC1 DER)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP192R1_ENABLED
pk_parse_keyfile_ec:"data_files/ec_prv.sec1.der":"NULL":0

Parse EC Key #1a (SEC1 DER, no optional part)
depends_on:POLARSSL_PEM_PARSE_C:POLARSSL_ECP_C:POLARSSL_ECP_DP_SECP256R1_ENABLED
pk_parse_keyfile_ec:"data_files/ec_prv.noopt.der":"NULL":0

Parse EC Key #2 (SEC1 PEM)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP192R1_ENABLED
pk_parse_keyfile_ec:"data_files/ec_prv.sec1.pem":"NULL":0

Parse
EC Key #3 (SEC1 PEM encrypted)
depends_on:MBEDTLS_DES_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP1
92R1_ENABLED:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_MD5_C
pk_parse_keyfile_ec:"data_files/ec_prv.sec1.pw.pem":"polar":0

Parse EC Key #4 (PKCS8 DER)
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP192R1_ENABLED
pk_parse_keyfile_ec:"data_files/ec_prv.pk8.der":"NULL":0

Parse EC Key #5 (PKCS8 PEM)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP192R1_ENABLED
pk_parse_keyfile_ec:"data_files/ec_prv.pk8.pem":"NULL":0

Parse EC Key #6 (PKCS8 encrypted DER)
depends_on:MBEDTLS_DES_C:MBEDTLS_SHA1_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP192R1_E
NABLED

pk_parse_keyfile_ec:"data_files/ec_prv.pk8.pw.der":"polar":0

Parse EC Key #7 (PKCS8 encrypted PEM)
depends_on:MBEDTLS_DES_C:MBEDTLS_SHA1_C:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP192R1_ENABLED
pk_parse_keyfile_ec:"data_files/ec_prv.pk8.pw.pem":"polar":0

Parse EC Key #8 (SEC1 PEM, secp224r1)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP224R1_ENABLED
pk_parse_keyfile_ec:"data_files/ec_224_prv.pem":"NULL":0

Parse
EC Key #9 (SEC1 PEM, secp256r1)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED
pk_parse_keyfile_ec:"data_files/ec_256_prv.pem":"NULL":0

Parse EC Key #10 (SEC1 PEM, secp384r1)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP384R1_ENABLED
pk_parse_keyfile_ec:"data_files/ec_384_prv.pem":"NULL":0

Parse EC Key #11 (SEC1 PEM, secp521r1)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP521R1_ENABLED
pk_parse_keyfile_ec:"data_files/ec_521_prv.pem":"NULL":0

Parse EC Key #12 (SEC1 PEM, bp256r1)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_BP256R1_ENABLED
pk_parse_keyfile_ec:"data_files/ec_bp256_prv.pem":"NULL":0

Parse EC Key #13 (SEC1 PEM, bp384r1)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_BP384R1_ENABLED
pk_parse_keyfile_ec:"data_files/ec_bp384_prv.pem":"NULL":0

Parse
EC Key #14 (SEC1 PEM, bp512r1)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_BP512R1_ENABLED
pk_parse_keyfile_ec:"data_files/ec_bp512_prv.pem":"NULL":0

Parse EC Key #15 (SEC1 DER, secp256k1, SpecifiedECDomain)
depends_on:MBEDTLS_PEM_PARSE_C:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256K1_ENABLED:MBEDTLS_PK_PARSE_EC_EXTENDED
pk_parse_keyfile_ec:"data_files/ec_prv.specdom.der":"NULL":0

Key ASN1 (Incorrect first tag)
pk_parse_key_rsa:"":"":MBEDTLS_ERR_PK_KEY_INVALID_FORMAT

Key ASN1 (RSAPrivateKey, incorrect version tag)
pk_parse_key_rsa:"300100":"":MBEDTLS_ERR_PK_KEY_INVALID_FORMAT

Key ASN1 (RSAPrivateKey, version tag missing)
pk_parse_key_rsa:"3000":"":MBEDTLS_ERR_PK_KEY_INVALID_FORMAT

Key ASN1 (RSAPrivateKey, invalid version)
pk_parse_key_rsa:"3003020101":"":MBEDTLS_ERR_PK_KEY_INVALID_FORMAT

Key ASN1 (RSAPrivateKey, correct version, incorrect tag)
pk_parse_key_rsa:"300402010000":"":MBEDTLS_ERR_PK_KEY_INVALID_FORMAT

Key ASN1 (RSAPrivateKey, values present, length mismatch)
pk_parse_key_rsa:"301c02010002010102010102010102010102010102010102010102010100":"":MBEDTLS_ERR_PK_KEY_INVALID_FORMAT

Key
ASN1 (RSAPrivateKey, values present, check_privkey fails)
pk_parse_key_rsa:"301b02010002010102010102010102010102010102010102010102010101":"":MBEDTLS_ERR_PK_KEY_INVALID_FORMAT
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
<ItemGroup Label="ProjectConfigurations">
<ProjectConfiguration Include="Debug|Win32">
<Configuration>Debug</Configuration>
<Platform>Win32</Platform>
</ProjectConfiguration>
<ProjectConfiguration Include="Debug|x64">
<Configuration>Debug</Configuration>
<Platform>x64</Platform>
</ProjectConfiguration>
<ProjectConfiguration Include="Release|Win32">
<Configuration>Release</Configuration>
<Platform>Win32</Platform>
</ProjectConfiguration>
<ProjectConfiguration Include="Release|x64">
<Configuration>Release</Configuration>
<Platform>x64</Platform>
</ProjectConfiguration>
</ItemGroup>
<PropertyGroup Label="Globals">
<ProjectGuid>{46CF2D25-6A36-4189-B59C-E4815388E554}</ProjectGuid>
<Keyword>Win32Proj</Keyword>
<RootNamespace>mbedTLS</RootNamespace>
</PropertyGroup>
<Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
<ConfigurationType>StaticLibrary</ConfigurationType>
<UseDebugLibraries>true</UseDebugLibraries>
<CharacterSet>Unicode</CharacterSet>

```
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
   <ConfigurationType>StaticLibrary</ConfigurationType>
   <UseDebugLibraries>true</UseDebugLibraries>
   <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>StaticLibrary</ConfigurationType>
   <UseDebugLibraries>false</UseDebugLibraries>
   <WholeProgramOptimization>true</WholeProgramOptimization>
   <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'"
 Label="Configuration">
   <ConfigurationType>StaticLibrary</ConfigurationType>
   <UseDebugLibraries>false</UseDebugLibraries>
   <WholeProgramOptimization>true</WholeProgramOptimization>
   <CharacterSet>Unicode</CharacterSet>
   <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')"
 Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
   <LinkIncremental>true</LinkIncremental>
```

```
    <IntDir>$(Configuration)\$(TargetName)\</IntDir>
  </PropertyGroup>
  <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
    <LinkIncremental>false</LinkIncremental>
    <IntDir>$(Configuration)\$(TargetName)\</IntDir>
  </PropertyGroup>
  <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
    <LinkIncremental>false</LinkIncremental>
    <IntDir>$(Configuration)\$(TargetName)\</IntDir>
  </PropertyGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
    <ClCompile>
      <PrecompiledHeader>
      </PrecompiledHeader>
      <WarningLevel>Level3</WarningLevel>
      <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_WINDOWS;_USRDLL;MBEDTLS_EXPORTS;%(PreprocessorDefi
nitions)</PreprocessorDefinitions>
      <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
      <CompileAs>CompileAsC</CompileAs>
    </ClCompile>
    <Link>
      <SubSystem>Windows</SubSystem>
      <GenerateDebugInformation>true</GenerateDebugInformation>
    </Link>
  </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
    <ClCompile>
      <PrecompiledHeader>
      </PrecompiledHeader>
      <WarningLevel>Level3</WarningLevel>
      <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_WINDOWS;_USRDLL;MBEDTLS_EXPORTS;%(PreprocessorDefi
nitions)</PreprocessorDefinitions>
      <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
      <CompileAs>CompileAsC</CompileAs>
    </ClCompile>
    <Link>
      <SubSystem>Windows</SubSystem>
      <GenerateDebugInformation>true</GenerateDebugInformation>
    </Link>
  </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
    <ClCompile>
      <WarningLevel>Level3</WarningLevel>
      <PrecompiledHeader>
       </PrecompiledHeader>
      <Optimization>MaxSpeed</Optimization>
```

```
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_WINDOWS;_USRDLL;MBEDTLS_EXPORTS;%(PreprocessorDef
initions)</PreprocessorDefinitions>
    <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Windows</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
  </Link>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_WINDOWS;_USRDLL;MBEDTLS_EXPORTS;%(PreprocessorDef
initions)</PreprocessorDefinitions>
    <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Windows</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
  </Link>
 </ItemDefinitionGroup>
 <ItemGroup>
HEADER_ENTRIES
 </ItemGroup>
 <ItemGroup>
SOURCE_ENTRIES
 </ItemGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
-----BEGIN EC PARAMETERS-----
BggqhkjOPQMBBw==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIDJyHSKbXEZVfkNftQF4eHeJVuXhGdaboa7w4RejL5uYoAoGCCqGSM49
AwEHoUQDQgAECckQhzQ+/CsWR6Bx3Tk4z7g+h4xz5xCl/GqW5VKREwybi1u2Ed1f
```

ENHU2nPiR4kentpeA5Q23+W04shaAM8Pcg==
-----END EC PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDBTCCAeegAwIBAgIBFjATBgkqhkiG9w0BAQowBqIEAgIA6jA7MQswCQYDVQQG
EwJOTDERMA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3Qg
Q0EwHhcNMTQwMTIwMTMzODE2WhcNMjQwMTE4MTMzODE2WjA0MQswCQYDVQQGEwJO
TDERMA8GA1UEChMIUG9sYXJTU0wxEjAQBgNVBAMTCWxvY2FsaG9zdDCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA3RGKn5m6sGjKKuo7am1Zl+1OyVTkDe7OoH2g
HqroDsK7E0DbihKOiRMkpcX1+tj1kNfIysvF/pMdr9oSI3NSeUYauqBXK3YWMbOo
r+c4mwiLY5k6CiXuRdIYWLq5kxrt1FiaYxs3/PcUCJ+FZUnzWTJt0eDobd5S7Wa0
qQvaQJUCAwEAAaOBkjCBjzAJBgNVHRMEAjAAMB0GA1UdDgQWBBTu88f1HxWlTUeJ
wdMiY7Lfp869UTBjBgNVHSMEXDBagBS0WuSls97SUva51aaVD+s+vMf9/6E/pD0w
OzELMAkGA1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NMMRkwFwYDVQQDExBQb2xh
clNTTCBUZXN0IENBggEAMBMGCSqGSIb3DQEBCjAGogQCAgDqA4IBAQDAog/jXydR
vDIugTzBXtfVK0CEX8iyQ4cVzQmXWSne8204v943K5D2hktSBkjdQUdcnVvVgLR6
te50jV89ptN/NofX+fo9fhSRN9vGgQVWzOOFiO0zcThy749pirJu1Kq5OJdthIyW
Pu0UCz5G0k3kTp0JPevGlsNc8S9Ak1tFuB0IPJjrbfODWHS2LDuO+dB6gpkNTdrj
88ogYtBsN4D5gsXBRUfobXokUwejBwLrD6XwyQx+0bMwSCxgHEhxvuUkx1vdlXGw
JG3aF92u8mIxoKSAPaPdqy930mQvmpUWcN5Y1IMbtEGoQCKMYgosFcazJpJcjnX1
o4Hl/lqjwCEG
-----END
CERTIFICATE-----
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 0 (0x0)
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=NL, O=PolarSSL, CN=PolarSSL Test CA
Validity
Not Before: Feb 12 14:44:00 2011 GMT
Not After : Feb 12 14:44:00 2021 GMT
Subject: C=NL, O=PolarSSL, CN=PolarSSL Test CA
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit):
00:c0:df:37:fc:17:bb:e0:96:9d:3f:86:de:96:32:
7d:44:a5:16:a0:cd:21:f1:99:d4:ec:ea:cb:7c:18:
58:08:94:a5:ec:9b:c5:8b:df:1a:1e:99:38:99:87:
1e:7b:c0:8d:39:df:38:5d:70:78:07:d3:9e:d9:93:
e8:b9:72:51:c5:ce:a3:30:52:a9:f2:e7:40:70:14:
cb:44:a2:72:0b:c2:e5:40:f9:3e:e5:a6:0e:b3:f9:
ec:4a:63:c0:b8:29:00:74:9c:57:3b:a8:a5:04:90:
71:f1:bd:83:d9:3f:d6:a5:e2:3c:2a:8f:ef:27:60:
c3:c6:9f:cb:ba:ec:60:7d:b7:e6:84:32:be:4f:fb:
58:26:22:03:5b:d4:b4:d5:fb:f5:e3:96:2e:70:c0:
e4:2e:bd:fc:2e:ee:e2:41:55:c0:34:2e:7d:24:72:
69:cb:47:b1:14:40:83:7d:67:f4:86:f6:31:ab:f1:

```
            79:a4:b2:b5:2e:12:f9:84:17:f0:62:6f:27:3e:13:
            58:b1:54:0d:21:9a:73:37:a1:30:cf:6f:92:dc:f6:
            e9:fc:ac:db:2e:28:d1:7e:02:4b:23:a0:15:f2:38:
            65:64:09:ea:0c:6e:8e:1b:17:a0:71:c8:b3:9b:c9:
            ab:e9:c3:f2:cf:87:96:8f:80:02:32:9e:99:58:6f:
            a2:d5
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints:
        CA:TRUE
      X509v3 Subject Key Identifier:
        B4:5A:E4:A5:B3:DE:D2:52:F6:B9:D5:A6:95:0F:EB:3E:BC:C7:FD:FF
      X509v3 Authority Key Identifier:
        keyid:B4:5A:E4:A5:B3:DE:D2:52:F6:B9:D5:A6:95:0F:EB:3E:BC:C7:FD:FF
        DirName:/C=NL/O=PolarSSL/CN=PolarSSL Test CA
        serial:00

  Signature Algorithm: sha1WithRSAEncryption
    b8:fd:54:d8:00:54:90:8b:25:b0:27:dd:95:cd:a2:f7:84:07:
    1d:87:89:4a:c4:78:11:d8:07:b5:d7:22:50:8e:48:eb:62:7a:
    32:89:be:63:47:53:ff:b6:be:f1:2e:8c:54:c0:99:3f:a0:b9:
    37:23:72:5f:0d:46:59:8f:d8:47:cd:97:4c:9f:07:0c:12:62:
    09:3a:24:e4:36:d9:e9:2c:da:38:d0:73:75:61:d7:c1:6c:26:
    8b:9b:e0:d5:dc:67:ed:8c:6b:33:d7:74:22:3c:4c:db:b5:8d:
    2a:ce:2c:0d:08:59:05:09:05:a6:39:9f:b3:67:1b:e2:83:e5:
    e1:8f:53:f6:67:93:c7:f9:6f:76:44:58:12:e8:3a:d4:97:e7:
    e9:c0:3e:a8:7a:72:3d:87:53:1f:e5:2c:84:84:e7:9a:9e:7f:
    66:d9:1f:9b:f5:13:48:b0:4d:14:d1:de:b2:24:d9:78:7d:f5:
    35:cc:58:19:d1:d2:99:ef:4d:73:f8:1f:89:d4:5a:d0:52:ce:
    09:f5:b1:46:51:6a:00:8e:3b:cc:6f:63:01:00:99:ed:9d:a6:
    08:60:cd:32:18:d0:73:e0:58:71:d9:e5:d2:53:d7:8d:d0:ca:
    e9:5d:2a:0a:0d:5d:55:ec:21:50:17:16:e6:06:4a:cd:5e:de:
    f7:e0:e9:54
-----BEGIN CERTIFICATE-----
MIIDhzCCAm+gAwIBAgIBADANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTEwMjEyMTQ0NDAwWhcNMjEwMjEyMTQ0NDAwWjA7MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDA3zf8F7vglp0/ht6WMn1EpRagzSHx
mdTs6st8GFgIlKXsm8WL3xoemTiZhx57wI053zhdcHgH057Zk+i5clHFzqMwUqny
50BwFMtEonILwuVA+T7lpg6z+exKY8C4KQB0nFc7qKUEkHHxvYPZP9al4jwqj+8n
YMPGn8u67GB9t+aEMr5P+1gmIgNb1LTV+/Xjli5wwOQuvfwu7uJBVcA0Ln0kcmnL
R7EUQIN9Z/SG9jGr8XmksrUuEvmEF/Bibyc+E1ixVA0hmnM3oTDPb5Lc9un8rNsu
KNF+AksjoBXyOGVkCeoMbo4bF6BxyLObyavpw/LPh5aPgAIynplYb6LVAgMBAAGj
gZUwgZIwDAYDVR0TBAUwAwEB/zAdBgNVHQ4EFgQUtFrkpbPe0lL2udWmlQ/rPrzH
/f8wYwYDVR0jBFwwWoAUtFrkpbPe0lL2udWmlQ/rPrzH/f+hP6Q9MDsxCzAJBgNV
BAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEZMBcGA1UEAxMQUG9sYXJTU0wgVGVz
dCBDQYIBADANBgkqhkiG9w0BAQUFAAOCAQEAuP1U2ABUkIslsCfdlc2i94QHHYeJ
```

SsR4EdgHtdciUI5I62J6Mom+Y0dT/7a+8S6MVMCZP6C5NyNyXw1GWY/YR82XTJ8H
DBJiCTok5DbZ6SzaONBzdWHXwWwmi5vg1dxn7YxrM9d0IjxM27WNKs4sDQhZBQkF
pjmfs2cb4oPl4Y9T9meTx/lvdkRYEug61Jfn6cA+qHpyPYdTH+UshITnmp5/Ztkf
m/UTSLBNFNHesiTZeH31NcxYGdHSme9Nc/gfidRa0FLOCfWxRlFqAI47zG9jAQCZ
7Z2mCGDNMhjQc+BYcdnl0lPXjdDK6V0qCg1dVewhUBcW5gZKzV7e9+DpVA==
-----END
CERTIFICATE-----
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDA0UszjREl+JklUyevaN8fb0Gp
13Dzb4pY3MCoJK15BWoeoUFAIVvuI0C8bRm/i1OO4BN9tSRrRjW+S89YbYy1C73P
UgKZSejjnEFA4chcSOKOhZlM6K7+Pcrcx+sdiDu1DheODMiSFhoxt+H6IUvBEGkI
5AWFu5MDP7wlU/AZfQIDAQAB
-----END PUBLIC KEY-----
-----BEGIN PUBLIC KEY-----
MIGbMBAGByqGSM49AgEGBSuBBAAjA4GGAAQAHeFC1U9p6wOO5LevnTygdzb9nPcZ
6zVNaYee5/PBNvsPv58I+Gvl+hKOwaBR0+bGQ+ha2o/6zzZjwmC9LIRLb1YAzujk
ip5l0Jyt2J8jXe4F87imRr5xXx9n1bQ04P8jofwH73dAGT5A7v9vO839dlqpFVAz
Uk/k8gX1RE4pLEwvasE=
-----END PUBLIC KEY-----
N =
A1D46FBA2318F8DCEF16C280948B1CF27966B9B47225ED2989F8D74B45BD36049C0AAB5AD0FF003553B
A843C8E12782FC5873BB89A3DC84B883D25666CD22BF3ACD5B675969F8BEBFBCAC93FDD927C7442B17
8B10D1DFF9398E52316AAE0AF74E594650BDC3C670241D418684593CDA1A7B9DC4F20D2FDC6F6634407
4003E211
E = 010001
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTIwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTMwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATrkzCJLznh
lhnsv1RXB9kfeaD+cIruPQ0cItBDGpdvD8xbBVvQci4+RG2RVUCSWRhkFYjSsUSM
0QHMQnBFlhw2o4GJMIGGMB0GA1UdDgQWBBTmVnUSF2MYwws/nCMv7b1wJVkDmjBX
BgNVHSMEUDBOgBTZTtbi+j0Sm/Zs/+gTkWdASpQzfqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTExggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgWsm+rHJgwUEyNm8EKbEds5yurpp5/3y5
PsvXJVDqxogCIQDUP0Jcl3A907CE2tPVXSgD6LQ6CPu19mixemPw60yijA==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTEwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTIwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATDE9LPlLPc
gZ3b0BchR/AkhNEP9HAavwYadJIyzoPo5edCVnboQH786jsZwZNZoC0gHDAhCmGc
IfRenISAoVuPo4GJMIGGMB0GA1UdDgQWBBTZTtbi+j0Sm/Zs/+gTkWdASpQzfjBX
BgNVHSMEUDBOgBSOSt6ePyMRT6PGMaIi7FqNX9MKtKEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTEwggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgYYF5AnRV7eh2hLD5Dz//pceMTKz9Ls46
E6DxvbfDHikCIFttlGrOCZVyS4ocsjuKIELVUX5qfygI0sn4kU3qCTs2

-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTAwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATZwR+WK6NB
F/7riFdN63c8hjYddZRR4lrzVNPwiBQxnnxwpPyrD9A6aPPmLc6SqGOJW4ZGVCco
IBze9RJVeiB9o4GJMIGGMB0GA1UdDgQWBBSOSt6ePyMRT6PGMaIi7FqNX9MKtDBX
BgNVHSMEUDBOgBQtxZSLJAkEz+2RKMQexM6EtsfgcqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA5ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgN//NqM0FrkrMjmxoeCY9DgxkH2R6sQ4d
NgtwCZAIqEICIBs4vupaVcuvni9tltbP26wi7c0FR+blZuo5DPIA3SVe
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDkwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTAwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAR6jlGKbJd5
hiDxN789gkOcwpyHI9wRwCrADAOwOkMePBPRlwGdm7mw7Z/EAmu26zRm/hcyrs4M
qk2LabDjPI9Xo4GJMIGGMB0GA1UdDgQWBBQtxZSLJAkEz+2RKMQexM6EtsfgcjBX
BgNVHSMEUDBOgBT6gyXHzPIPYc1Vr1aGiLLeMh4HpqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA4ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgP7S8vFstfUBdNe6ym5GYG5Q+aBVEKqRs
fVW7HNUktSYCIQDo6Jua6o/DJbrpq4qYWq5gv4yGyzPTN+3IaKrEICdaaw==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDgwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDkwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAR7ZB16+t6E
sfahGyKUGJW5mezkzjdaYvc4lbJaKNRwFRfc3F/fmNOSsUFSg/F0N+vUE+doKiPC
8wRwLzvm4s+5o4GJMIGGMB0GA1UdDgQWBBT6gyXHzPIPYc1Vr1aGiLLeMh4HpjBX
BgNVHSMEUDBOgBS40mLt93U8Sh8ZGiDVAhRSiBPcXqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA3ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgO4el1ZPhlIli/qNR2SIEiuvs5Mmy868i
N2Rv5X/VxIECIA/8rUALQxW38XSdBVX3e/jzu7ju47n1YwEqD9K9WdVv
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDcwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDgwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAARpQeQ/YGQj
nl7Szo6WStJ1u7xunTL5jBkXH8aAVSm0qiX4AD/7YPxa5EnGzZdLTn25vQVnfQAG
pMx8P1lYiGYCo4GJMIGGMB0GA1UdDgQWBBS40mLt93U8Sh8ZGiDVAhRSiBPcXjBX
BgNVHSMEUDBOgBREq5J3toJPxZ3O+ssJ5vkkU0RJE6EzpDEwLzELMAkGA1UEBhMC

VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA2ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhANwGf+F4a+kmXWz8UjSpRkaToTV6EFWw
/Tjzj0tQhDoAAiEA19RxeWOVBBpM6LOHg6v5Lf54YN1snkLf+sEXyZCuWQQ=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDYwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDcwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASNOj4d4MEA
7p/3miijqG4ToE4opKPAm+3BTIGrJTYT14++TSiUICl0ASXj+xeUcLMIaXTN042s
LsHxpShzQaL0o4GJMIGGMB0GA1UdDgQWBBREq5J3toJPxZ3O+ssJ5vkkU0RJEzBX
BgNVHSMEUDBOgBSjovYaC/m6Li9Tp0V9iZRs9267Q6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA1ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAKGcf+c442c/XiwubbaiQvsoZ7EoVxuM
oKmia0gPyBNkAiEA83asjJ5FDXQuLyZpczviXrbmqgCPOfYadtvkc0cxMis=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDUwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDYwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASA9qWoAUHr
nn+3kxyNrjPJk82WDLimW21RN51uxpobadv8YgGEDRdP+Ok+uRqQSUsA6ZXfF3iG
r2GjfQ3wMDH8o4GJMIGGMB0GA1UdDgQWBBSjovYaC/m6Li9Tp0V9iZRs9267QzBX
BgNVHSMEUDBOgBTXh06MAV9S4l4lG1TKOrKRBh4qn6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA0ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgcjZNFWJtlDmoPZbAxqsGczRYK0lfPgu6
g1H7pp0ce+wCIDj9BRZM2OB9EF0e+MDKGjyZGfvfrL6Ir47x/KrM6H8T
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDQwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDUwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQEdT0OFf5G
UcrgX2XllCyJzP94NZ464GsgB6psNLsDeL+j7AU+oJy7VLvW/lHh3ODgl08Z9bhq
LFBmNjnHbm8Qo4GJMIGGMB0GA1UdDgQWBBTXh06MAV9S4l4lG1TKOrKRBh4qnzBX
BgNVHSMEUDBOgBQox4F1NsZunlsduoGvzIgRSYfB36EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAzggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAIW++zqDZlLLUk/emePohdNOp5JO3wS9
XvkBJ6Wua7GBAiAdx+EKmdjVrwnzrQltTgnmSfGMXhKNYifK3uD83W3pcQ==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDMwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDQwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQUXDgcUVNT

9hovbZE5HL6rjOb7C55wEuWKThV/CcZ4rWrXx7VXHYdD/R3aDA7JSvYpm2sTok4i
sblDzhZM/GDNo4GJMIGGMB0GA1UdDgQWBBQox4F1NsZunlsduoGvzIgRSYfB3zBX
BgNVHSMEUDBOgBQApzZdtBdD3dLxouQpr/aDiVttd6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAyggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgAkiNhqFAZXSUWEDK91OZvQGdeZOtd6mC
+Wv3fGk3t28CIEKOwidkUTUaiPdZ4efmAr+CEeGzdq27ob2S+nqqHqgV
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDIwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDMwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQRDXDNIi1p
ereudhqwa2LslXgsxnB63Hu5y5lg+1WPruIYPzD/Ho0APveVdzFLVji19+bE4+tF
PYL1SpsN1WfWo4GJMIGGMB0GA1UdDgQWBBQApzZdtBdD3dLxouQpr/aDiVttdzBX
BgNVHSMEUDBOgBT5RCgQ0AlZTQbfFB2+6+w0XRvydaEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAxggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAOnd+7bAofkHVa4KFNjv3TCegw1lrhuM
8Of8wgvrTEGoAiEAsS8iKMpSfXH4D0egg4gLamE6akde965rDtySU+ve9lg=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDEwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDIwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQWHpv1i6lf
wvNPOP5ka6S0n55EvzoaYK6pbTXP6yMOW/4XZSPKx5Zoq4FMe0cKzGIIFL1rzj1V
2czYB+qvLhyio4GJMIGGMB0GA1UdDgQWBBT5RCgQ0AlZTQbfFB2+6+w0XRvydTBX
BgNVHSMEUDBOgBSh3uHkX5nj86yFEFwjscSWM40P+qEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAI7unGW/gr9tOc3i+dF5N815srgh+FrX
oj9Et74EcSpTAiBubv+vOH0DE0gmYI11HeAIgutWqqMIC72dZlwTF/Vi3g==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB3jCCAYWgAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDAwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQznn9zHHwL
GO8VR4W9V7vMlxCdoojzEOiX5Y6JtPtFOz866ueHY6zoN0/mJ6DnqnSXilJIUUeW
6eGfqmka7nxko4GRMIGOMB0GA1UdDgQWBBSh3uHkX5nj86yFEFwjscSWM40P+jBf
BgNVHSMEWDBWgBQlFYvU5WboI4fcdPoiQs8/fPHZraEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggkA/KCWhcqToHAw
DAYDVR0TBAUwAwEB/zAKBggqhkjOPQQDAgNHADBEAiBasbuinP+pJTU4oDCVD8zQ
1rJBDSOKIEyWu84/D6Hj6wIgVMPUoO01bPhzllAa/gW8Xk/daey09SBgN3AT9pWU
TDA=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----

MIIBpTCCAUugAwIBAgIJAPygloXKk6BwMAoGCCqGSM49BAMCMC8xCzAJBgNVBAYT
AlVLMREwDwYDVQQKDAhtYmVkIFRMUzENMAsGA1UEAwwEQ0EwMDAeFw0xNzA2MjIx
MTUwMzJaFw0yNzA2MjMxMTUwMzJaMC8xCzAJBgNVBAYTAlVLMREwDwYDVQQKDAht
YmVkIFRMUzENMAsGA1UEAwwEQ0EwMDBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IA
BFW41/qAwAPpy+Txdc7PKmzZsq9CPiujKU4vpF1ekXnGx2HP420QobwBVVWhkzRm
LwdboH2j65dcCKjQ7mv/dxKjUDBOMB0GA1UdDgQWBBQlFYvU5WboI4fcdPoiQs8/
fPHZrTAfBgNVHSMEGDAWgBQlFYvU5WboI4fcdPoiQs8/fPHZrTAMBgNVHRMEBTAD
AQH/MAoGCCqGSM49BAMCA0gAMEUCIQC7iRcVzwMyfVK5imirJ7MqJQ04euH4CLOt
IZ+SNfaERAIgSU0MWFDosVEIpg8YMqIHeF7Mg4ZyH6+fGazJgVLttUY=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDijCCAnKgAwIBAgIBKzANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTQwNDA5MDg0NDM5WhcNMjQwNDA2MDg0NDM5WjA0MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxEjAQBgNVBAMTCWxvY2FsaG9zdDCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBAMFNo93nzR3RBNdJcriZrA545Do8Ss86ExbQWuTN
owCIp+4ea5anUrSQ7y1yej4kmvy2NKwk9XfgJmSMnLAofaHa6ozmyRyWvP7BBFKz
NtSj+uGxdtiQwWG0ZlI2oiZTqqt0Xgd9GYLbKtgfoNkNHC1JZvdbJXNG6AuKT2kM
tQCQ4dqCEGZ9rlQri2V5kaHiYcPNQEkI7mgM8YuG0ka/0LiqEQMef1aoGh5EGA8P
hYvai0Re4hjGYi/HZo36Xdh98yeJKQHFkA4/J/EwyEoO79bex8cna8cFPXrEAjya
HT4P6DSYW8tzS1KW2BGiLICIaTla0w+w3lkvEcf36hIBMJcCAwEAAaOBnzCBnDAJ
BgNVHRMEAjAAMB0GA1UdDgQWBBSlBehkuNzfYA9QEk1gqGSvTYtDkzBjBgNVHSME
XDBagBS0WuSls97SUva51aaVD+s+vMf9/6E/pD0wOzELMAkGA1UEBhMCTkwxETAP
BgNVBAoTCFBvbGFyU1NMMRkwFwYDVQQDExBQb2xhclNTTCBUZXN0IENBggEAMAsG
A1UdDwQEAwIFIDANBgkqhkiG9w0BAQUFAAOCAQEAqreLAIuxeLGKbhoEROYRqXxO
ndaC6uDcpxhgmEW7B2DW6ZtX8155v3ov61MuMas8fEQjD5STDP9qERxNTePnhW3m
kDZd2jUBE3ioHhTBv47i1PYU+DRe42kY6z0jUmNPK8TsTKfdbqTGXg9THe1KYB7q
hdljqGS08IgBl/q2lK2OOSycu27xhfb9Mo0BcLBab92WgyBu+cFPQsKiL4mD7QyJ
+73Ndb21EuANUjsRDQ3NPklssJcyJB2v85eekwk1acZUG21no3wdTvjxhVE/Xrdz
zUP9WkvAVfUrwGjUzG4YHE8wkHO7xKbKixNt+nQmDhe+tHVbztZjVwFJ8010gg==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIICFzCCAYCgAwIBAgIJAJsTzkylb95SMA0GCSqGSIb3DQEBBQUAMD8xCzAJBgNV
BAYTAkdCMRIwEAYDVQQHDAlDYW1icmlkZ2UxHDAaBgNVBAoME0RlZmF1bHQgQ29t
cGFueSBMdGQwHhcNMTUwNTEyMTAzNjU1WhcNMTgwNTExMTAzNjU1WjA/MQswCQYD
VQQGEwJHQjESMBAGA1UEBwwJQ2FtYnJpZGdlMRwwGgYDVQQKDBNEZWZhdWx0IENv
bXBhbnkgTHRkMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC9nxYOSbha/Ap4
6rACrOMH7zfDD+0ZEHhbO0bgGRjc5ElvOaNuD321y9TnyAx+JrqPp/lFrAgNiVo1
HPurPHfcJ+tNBUgBHboWGNENNaf9ovwFPawsBzEZraGnDaqVPEFcIsUQPVqO1lrQ
CHLUjtqo1hMZDqe/Web0Mw9cZrqOaQIDAQABoxswGTAJBgNVHRMEAjAAMAwGA1Ud
DwQFAwMH4IAwDQYJKoZIhvcNAQEFBQADgYEAJ0NS2wUbgRelK0qKxrR2Ts6jVYEH
bmykx3GHjFyKpscDIn2vNyyB7ygfFglZPcw+2mn3xuVIwOV/mWxFvKHk+j2WrTQL
tDqSC5BhFoR01veFu07JdEYvz+I+NCL5z0IGWXkUrk235Wl4w4WMZDnXTqncMNEk
fLtpo9y79XD00QY=
-----END CERTIFICATE-----
mbedtls_md2 Test vector RFC1319 #1
md2_text:"":"8350e5a3e24c153df2275c9f80692773"

mbedtls_md2 Test vector RFC1319 #2
md2_text:"a":"32ec01ec4a6dac72c0ab96fb34c0b5d1"

mbedtls_md2 Test vector RFC1319 #3
md2_text:"abc":"da853b0d3f88d99b30283a69e6ded6bb"

mbedtls_md2 Test vector RFC1319 #4
md2_text:"message digest":"ab4f496bfb2a530b219ff33031fe06b0"

mbedtls_md2 Test vector RFC1319 #5
md2_text:"abcdefghijklmnopqrstuvwxyz":"4e8ddff3650292ab5a4108c3aa47940b"

mbedtls_md2 Test vector RFC1319 #6
md2_text:"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789":"da33def2a42df13975352846c30338cd"

mbedtls_md2 Test vector RFC1319 #7
md2_text:"12345678901234567890123456789012345678901234567890123456789012345678901234567890":"d5976f79d83d3a0dc9806c3c66f3efd8"

mbedtls_md4 Test vector RFC1320 #1
md4_text:"":"31d6cfe0d16ae931b73c59d7e0c089c0"

mbedtls_md4 Test vector RFC1320 #2
md4_text:"a":"bde52cb31de33e46245e05fbdbd6fb24"

mbedtls_md4 Test vector RFC1320 #3
md4_text:"abc":"a448017aaf21d8525fc10ae87aa6729d"

mbedtls_md4
Test vector RFC1320 #4
md4_text:"message digest":"d9130a8164549fe818874806e1c7014b"

mbedtls_md4 Test vector RFC1320 #5
md4_text:"abcdefghijklmnopqrstuvwxyz":"d79e1c308aa5bbcdeea8ed63df412da9"

mbedtls_md4 Test vector RFC1320 #6
md4_text:"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789":"043f8582f241db351ce627e153e7f0e4"

mbedtls_md4 Test vector RFC1320 #7
md4_text:"12345678901234567890123456789012345678901234567890123456789012345678901234567890":"e33b4ddc9c38f2199c3e7b164fcc0536"

mbedtls_md5 Test vector RFC1321 #1
md5_text:"":"d41d8cd98f00b204e9800998ecf8427e"

mbedtls_md5 Test vector RFC1321 #2
md5_text:"a":"0cc175b9c0f1b6a831c399e269772661"

mbedtls_md5 Test vector RFC1321 #3
md5_text:"abc":"900150983cd24fb0d6963f7d28e17f72"

mbedtls_md5 Test vector RFC1321 #4
md5_text:"message digest":"f96b697d7cb7938d525a2f31aaf161d0"

mbedtls_md5 Test vector RFC1321 #5
md5_text:"abcdefghijklmnopqrstuvwxyz":"c3fcd3d76192e4007dfb496cca67e13b"

mbedtls_md5
Test vector RFC1321 #6
md5_text:"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789":"d174ab98d277d9f5a5611c2c9f419d9f"

mbedtls_md5 Test vector RFC1321 #7
md5_text:"12345678901234567890123456789012345678901234567890123456789012345678901234567890":"57edf4a22be3c955ac49da2e2107b67a"

mbedtls_ripemd160 Test vector from paper #1
ripemd160_text:"":"9c1185a5c5e9fc54612808977ee8f548b2258d31"

mbedtls_ripemd160 Test vector from paper #2
ripemd160_text:"a":"0bdc9d2d256b3ee9daae347be6f4dc835a467ffe"

mbedtls_ripemd160 Test vector from paper #3
ripemd160_text:"abc":"8eb208f7e05d987a9b044a8e98c6b087f15a0bfc"

mbedtls_ripemd160 Test vector from paper #4
ripemd160_text:"message digest":"5d0689ef49d2fae572b881b123a85ffa21595f36"

mbedtls_ripemd160 Test vector from paper #5
ripemd160_text:"abcdefghijklmnopqrstuvwxyz":"f71c27109c692c1b56bbdceb5b9d2865b3708dbc"

mbedtls_ripemd160 Test vector from paper #6
ripemd160_text:"abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq":"12a053384a9c0c88e405a06c27dcf49ada62eb2b"

mbedtls_ripemd160
Test vector from paper #7
ripemd160_text:"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789":"b0e20b6e3116640286ed3a87a5713079b21f5189"

mbedtls_ripemd160 Test vector from paper #8
ripemd160_text:"1234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890":"9b752e45573d4b39f4dbd3323cab82bf63326bfb"

MD2 Selftest
md2_selftest:

MD4 Selftest
md4_selftest:

MD5 Selftest
md5_selftest:

RIPEMD160 Selftest
ripemd160_selftest:
-----BEGIN CERTIFICATE-----
MIIB8jCCAVugAwIBAgIETZt8+zANBgkqhkiG9w0BAQUFADBCMUAwPgYDVQQDDDdP
cGVuVlBOIFdlYiBDQSAyMDExLjA0LjA1IDIwOjMzOjI3IFVUQyBhc2RlbW8ueW9u
YW4ubmV0MB4XDTE0MDcyOTAzNTMzM1oXDTI0MDgwMjAzNTMzM1owFzEVMBMGA1UE
AwwMZHcueW9uYW4ubmV0MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDHYW8q
ZZ/HIIlU8j/YIyTh3h59JcJF0Es7RsPg25QVJkDkfhMn6l15f2neB2KPLKxCLpLD
ozYD4s/If8aq74A1C2vvOLo/Gq1erNS4b9IS5xLs3Lu643XGxS93Rf6jrsGa8lfb
Wa7DsQrp7FLT5GApwCp6CebmZq7jEImj0pDFRwIDAQABoyAwHjAJBgNVHRMEAjAA
MBEGCWCGSAGG+EIBAQQEAwIGQDANBgkqhkiG9w0BAQUFAAOBgQAS1Ulo7iBABpm/
S23mCnIFRY1+eFfYg4h8EiK9f8kWDwduXSYGVUqRHqh4LcNSdTOIaSEG4RGyV/EA
5RfTviaQ9PxPiSFegNja8/aHel/nORfsEk4rwBCPGKDveL5KYhAtyAs865ZzLtv+
kEkfhaTgrBIikwlnquoX5UHOdL/iaw==
-----END CERTIFICATE-----
-----BEGIN EC PARAMETERS-----
BggqhkjOPQMBBw==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIKb966FXMh8cFQt3sVpmcrh2/3yaGiLMwz+/XGKGMJ+2oAoGCCqGSM49
AwEHoUQDQgAE65MwiS854ZYZ7L9UVwfZH3mg/nCK7j0NHCLQQxqXbw/MWwVb0HIu
PkRtkVVAklkYZBWI0rFEjNEBzEJwRZYcNg==
-----END EC PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDwjCCAaqgAwIBAgIBEDANBgkqhkiG9w0BAQsFADBIMQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxJjAkBgNVBAMTHVBvbGFyU1NMIFRlc3QgSW50ZXJt
ZWRpYXRlIENBMB4XDTEzMDkyNDE2MTIyNFoXDTIzMDkyMjE2MTIyNFowNDELMAkG
A1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NMMRIwEAYDVQQDEwlsb2NhbGhvc3Qw
WTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQcbffp2qXqoZyychmoCRxzrd4Vu96m
47NPBehtEC46aTeXgDnBdf++znABrAtfXBRNQz8ARIeYBmskr22rlKjyo4GVMIGS
MAkGA1UdEwQCMAAwHQYDVR0OBBYEFNIK06V3H85VsFxGoo5zbL+hYCa7MGYGA1Ud
IwRfMF2AFDh32Gt3nCh3gotO2BupHveUFrcOoUKkQDA+MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0GC
AQ4wDQYJKoZIhvcNAQELBQADggIBADRoQ5fHKw+vkl0D3aqLX1XrZidb+25AWbhr
FYXdaskN219PrXBL3cV8x5tK6qsPKSyyw1lue80OmhXs/w7PJkOHHUSWRnmTv7lr
8Us3Zr/yOF/VVqzdGs7DlOTpyzEBdugI9uar/aCqHDoltN8wOduOoQB9aojYpROj
+gjlEO0mgt/87XpjYOig1o0jv44QYDQZQzpj1zeIn6WMe6xk9YDwCLMjRIpg++c7
QyxvcEJTn80wX1SaEBM2gau97G7bORLMwBVkMT4oSY+iKYgpPpawOnMJbqUP73Dm

yfJExDdrW/BbWZ/vKIcSqSZIbkHdkNjUDVHczyVwQxZxzvLFw/B1k9s7jYFsi5eK

TNAdXFa4et1H2sd+uhu24GxsjmJioDrftixcgzPVBjDCjH8QWkBEX292WJ58on0e
deWLpZUnzPdE1B4rsiPw1Vg28mGgr2O1xgBQr/fx6A+8ItNTzAXbZfEcult9ypwM
0b6YDNe5IvdKk8iwz3mof0VNy47K6xoCaE/fxxWkjoXK8x2wfswGeP2QgUzQE93b
OtjdHpsG1c7gIVFQmKATyAPUz4vqmezgNRleXU0oL0PYtoCmKQ51UjNMUfmO9xCj
VJaNa2iTQ5Dgic+CW4TYAgj5/9g9X3WfwnDNxrZ0UxxawGElczHXqbrNleTtPaKp
a8Si6UK5
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEATCCA4egAwIBAgIBDjAKBggqhkjOPQQDAjA+MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EwHhcN
MTMwOTI0MTU1NTE0WhcNMjMwOTIyMTU1NTE0WjBIMQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxJjAkBgNVBAMTHVBvbGFyU1NMIFRlc3QgSW50ZXJtZWRp
YXRlIENBMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAo1Oc8nr6fMTq
vowV+CpC55i5BZGFGc50Eb4RLBSRTH1e7JepdFjAVbBtyQRJSiY1ja0tgLQDDKZR
wfEI+b4azse460InPHv7C1TN0upXlxuj6m9B1llP+sBaM7WBC6dVfPO+jVMIxgkF
CaBCLhhdK1Fjf8HjkT/PkctWnho8NTwivc9+nqRZjXe/eIcqm5HwjDDhu+gz+o0g
Vz9MfZNi1JyCrOyNZcy+cr2QeNnNVGnFq8xTxtu6dLunhpmLFj2mm0Vjwa7Ypj5q

AjpqTMtDvqbRuToyoyzajhMNcCAf7gwzIupJJFVdjdtgYAcQwzikwF5HoITJzzJ2
qgxF7CmvGZNb7G99mLdLdhtclH3wAQKHYwEGJo7XKyNEuHPQgB+e0cg1SD1HqlAM
uCfGGTWQ6me7Bjan3t0NzoTdDq6IpKTesbaY+/9e2xn8DCrhBKLXQMZFDZqUoLYA
kGPOEGgvlPnIIXAawouxCaNYEh5Uw871YMSPT28rLdFr49dwYOtDg9foA8hDIW2P
d6KXbrZteesvA1nYzEOs+3AjrbT79Md2W8Bz9bqBVNlNOESSqm4kiCJFmslm/6br
Np0MSQd+o22PQ4xRtmP6UsTfU0ueiMpYc8TYYhMbfnfFyo4m707ebcflPbBEN2dg
updQ66cvfCJB0QJt9upafY0lpdV1qUkCAwEAAaOBoDCBnTAdBgNVHQ4EFgQUOHfY
a3ecKHeCi07YG6ke95QWtw4wbgYDVR0jBGcwZYAUnW0gJEkBPyvLeLUZvH4kydv7
NnyhQqRAMD4xCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UE
AxMTUG9sYXJzc2wgVGVzdCBFQyBDQYIJAMFD4n5iQ8zoMAwGA1UdEwQFMAMBAf8w
CgYIKoZIzj0EAwIDaAAwZQIxAPyE+u+eP7gRrSFjQicmpYg8jiFUCYEowWY2zuOG
i1HXYwmpDHfasQ3rNSuf/gHvjwIwbSSjumDk+uYNci/KMELDsD0MFHxZhhBc9Hp9
Af5cNR8KhzegznL6amRObGGKmX1F
-----END CERTIFICATE-----
-----BEGIN PUBLIC KEY-----
ME4wEAYHKoZIzj0CAQYFK4EEACEDOgAEFpOikPfwtXH+K0HV2EsBMnYx9Khg+ZX6
MywJf1QZK7EPABE/Kv+xPBokzkSRRXGpVECuAUoAy/c=
-----END PUBLIC KEY-----
-----BEGIN CERTIFICATE REQUEST-----
MIICgTCCAWkCAQAwPDELMAkGA1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NMMRow
GAYDVQQDExFQb2xhclNTTCBTZXJ2ZXIgMTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAKkCHz1AatVVU4v9Nu6CZS4VYV6Jv7joRZDb7ogWUtPxQ1BHlhJZ
ZIdr/SvgRvlzvt3PkuGRW+1moG+JKXlFgNCDatVBQ3dfOXwJBEeCsFc5cO2j7BUZ
HqgzCEfBBUKp/UzDtN/dBh9NEFFAZ3MTD0D4bYElXwqxU8YwfhU5rPla7n+SnqYF
W+cTl4W1I5LZ1CQG1QkliXUH3aYajz8JGb6tZSxk65Wb3P5BXhem2mxbacwCuhQs
FiScStzN0PdSZ3PxLaAj/X70McotcMqJCwTbLqZPcG6ezr1YieJTWZ5uWpJl4og/
DJQZo93l6J2VE+0p26twEtxaymsXq1KCVLECAwEAAaAAMA0GCSqGSIb3DQEBDQUA
A4IBAQBH78JrIboWUlOiUzEwxuYkaRBr22DfdSHlNVjnenrTsSsSdfPenfrUbs42

```
NfzhJtvLBnDMs9olsiyPNKZnROmjl/4Da5ScVBfdA7oSImwdsaL0krAju8lJosy7
ypqNejQQDgjL00HkaVyqjnEWY68enAkaK64suQ4w0pkGmtdZyg0nBiH1VI72PcPR
Fu2wxSkvvYj+BcHVAY/GWRMTHw1mkmsQna7AsZ1MFIF3ycIW5Fom6d0wpB6clJ3M
vNTBc7kZIR1BQyblyU96acesxJURJn5xO9Yf9OSsTbd7Xm5xK6DpQWxFFEgdVtir
hSAqtp54nVnLe4QihmVAlM8zt2ON
-----END CERTIFICATE REQUEST-----
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 9 (0x9)
    Signature Algorithm: md2WithRSAEncryption
    Issuer: C=NL, O=PolarSSL, CN=PolarSSL Test CA
    Validity
      Not Before: Jul 12 10:56:59 2009 GMT
      Not After : Jul 12 10:56:59 2011 GMT
    Subject: C=NL, O=PolarSSL, CN=PolarSSL Cert MD2
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (2048 bit)
        Modulus (2048 bit):
          00:dc:13:74:81:c6:12:f6:67:5d:a1:66:72:ed:dc:
          79:b6:58:5c:32:58:b3:d4:14:fd:6c:02:61:9e:0b:
          99:46:63:a3:0a:41:d4:42:33:21:e6:ed:43:07:5a:
          1d:a2:3b:64:29:a8:2a:c1:66:28:00:59:d8:0c:49:
          2d:30:b7:3d:8c:bb:60:62:31:83:27:7f:4b:95:92:
          2e:a0:d6:c6:84:94:4b:b3:e4:a6:cc:ff:32:3a:c5:
          ec:4c:c9:24:58:bf:b3:33:77:6a:b5:17:8b:02:10:
          29:8e:95:aa:91:60:17:43:42:87:a8:7c:da:09:83:
          98:9d:7a:65:5e:20:52:07:2e:65:a5:31:fd:d9:74:
          1e:00:c9:ae:9d:81:56:8b:08:0a:f5:1e:9c:dc:a2:
          5e:6c:db:ff:11:83:15:f4:d1:24:57:9b:0f:eb:35:
          c9:f1:aa:46:4e:74:7f:fe:1d:b0:91:1f:89:4a:84:
          cb:df:75:e3:cd:77:82:62:09:e5:9f:6d:29:de:2e:
          25:d8:48:b6:20:be:51:97:4c:2d:20:65:2d:2a:50:
          9e:24:5d:72:95:e0:a2:06:41:8c:61:e4:50:57:74:
          96:b1:29:b5:a1:88:37:f1:5c:9e:b2:9e:8e:83:8d:
          72:3b:b5:5c:fe:bb:12:89:72:5c:a1:f9:d8:18:29:
          b2:27
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints:
        CA:FALSE
      X509v3 Subject Key Identifier:
        B7:51:D4:E5:20:D5:45:54:F4:C5:51:1B:E0:82:B5:61:05:AF:9B:B6
      X509v3 Authority Key Identifier:
        keyid:CF:22:31:27:91:D8:C2:54:FF:1E:DA:D9:EE:8A:C5:89:32:AD:0C:21
```

Signature Algorithm: md2WithRSAEncryption
28:5a:dd:48:fb:ec:80:fe:de:b7:20:c0:4c:05:a9:4b:51:e9:
a7:d1:4b:5e:76:42:d2:5d:9a:14:19:3b:cb:f9:91:d7:0f:11:
c9:cd:dd:00:8b:2c:76:73:22:a0:19:49:81:63:40:30:48:27:
62:90:ca:b8:dc:33:35:b3:4b:58:ca:dc:07:66:87:2e:ea:44:
2a:6a:13:67:7a:32:5e:48:1d:88:88:c5:70:e6:e7:ec:1b:2f:
a7:f4:61:71:29:f6:66:93:30:60:7e:b3:4c:01:c8:2c:53:ce:
00:11:ec:bf:f6:f2:ce:51:97:d8:ed:ed:dc:c9:6b:b8:19:15:
c8:9a:61:6d:12:9a:99:25:d8:03:1d:a6:4c:20:a5:f8:46:a3:
05:32:bb:1a:8e:1a:65:0d:f3:13:35:1d:6f:73:28:31:12:d7:
c4:9e:73:a0:a7:ce:82:25:d1:40:e8:1b:77:60:f3:3e:81:7f:
19:ee:cf:97:4d:c8:c3:35:9b:72:98:3b:c3:35:43:14:0a:04:
21:7b:f7:db:e6:5f:ce:21:d1:ce:bf:b7:ef:c1:63:21:c2:78:
e1:37:aa:b1:e0:31:b3:b6:63:4c:fd:66:c8:e6:cf:f8:d9:97:
2f:cf:92:81:3f:d4:bf:ec:e2:ad:6e:39:c7:a6:a8:e0:32:b0:
2e:0d:e1:30
-----BEGIN CERTIFICATE-----
MIIDPzCCAiegAwIBAgIBCTANBgkqhkiG9w0BAQIFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MDkwNzEyMTA1NjU5WhcNMTEwNzEyMTA1NjU5WjA8MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxGjAYBgNVBAMTEVBvbGFyU1NMIENlcnQgTUQyMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3BN0gcYS9mddoWZy7dx5tlhcMliz
1BT9bAJhnguZRmOjCkHUQjMh5u1DB1odojtkKagqwWYoAFnYDEktMLc9jLtgYjGD
J39LlZIuoNbGhJRLs+SmzP8yOsXsTMkkWL+zM3dqtReLAhApjpWqkWAXQ0KHqHza
CYOYnXplXiBSBy5lpTH92XQeAMmunYFWiwgK9R6c3KJebNv/EYMV9NEkV5sP6zXJ
8apGTnR//h2wkR+JSoTL33XjzXeCYgnln20p3i4l2Ei2IL5Rl0wtIGUtKlCeJF1y
leCiBkGMYeRQV3SWsSm1oYg38Vyesp6Og41yO7Vc/rsSiXJcofnYGCmyJwIDAQAB
o00wSzAJBgNVHRMEAjAAMB0GA1UdDgQWBBS3UdTlINVFVPTFURvggrVhBa+btjAf
BgNVHSMEGDAWgBTPIjEnkdjCVP8e2tnuisWJMq0MITANBgkqhkiG9w0BAQIFAAOC
AQEAKFrdSPvsgP7etyDATAWpS1Hpp9FLXnZC0l2aFBk7y/mR1w8Ryc3dAIssdnMi
oBlJgWNAMEgnYpDKuNwzNbNLWMrcB2aHLupEKmoTZ3oyXkgdiIjFcObn7Bsvp/Rh
cSn2ZpMwYH6zTAHILFPOABHsv/byzlGX2O3t3MlruBkVyJphbRKamSXYAx2mTCCl
+EajBTK7Go4aZQ3zEzUdb3MoMRLXxJ5zoKfOgiXRQOgbd2DzPoF/Ge7Pl03IwzWb
cpg7wzVDFAoEIXv32+ZfziHRzr+378FjIcJ44TeqseAxs7ZjTP1myObP+NmXL8+S
gT/Uv+zirW45x6ao4DKwLg3hMA==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIICHTCCAaSgAwIBAgIBEjAJBgcqhkjOPQQBMD4xCzAJBgNVBAYTAk5MMREwDwYD
VQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBFQyBDQTAeFw0x
MzA5MjQxNjIxMjdaFw0yMzA5MjIxNjIxMjdaMDQxCzAJBgNVBAYTAk5MMREwDwYD
VQQKEwhQb2xhclNTTDESMBAGA1UEAxMJbG9jYWxob3N0MFkwEwYHKoZIzj0CAQYI
KoZIzj0DAQcDQgAEN8xW2XYJHlpyPsdZLf8gbu58+QaRdNCtFLX3aCJZYpJO5QDY
IxH/6i/SNF1dFr2KiMJrdw1VzYoqDvoByLTt/6OBnTCBmjAJBgNVHRMEAjAAMB0G
A1UdDgQWBBRQYaWP1AfZ14IBDOVlf4xjRqcTvjBuBgNVHSMEZzBlgBSdbSAkSQE/
K8t4tRm8fiTJ2/s2fKFCpEAwPjELMAkGA1UEBhMCTkwxETAPBgNVBAoTCFBvbGFy
U1NMMRwwGgYDVQQDExNQb2xhcnNzbCBUZXN0IEVDIENBggkAwUPifmJDzOgwCQYH
KoZIzj0EAQNoADBlAjEAyjvzRWtxbXvkoYTYSQY9gFBpP7/wTZ2q6FbRiAuZULFt

```
lc0PMPDfVZChgA6iDH+BAjBdkOb73f2pOwZpMRqrOgqSynbt2uWY87mC5lRlNEoR
WXEv1AzIeBCv+81DN1Iuu4w=
-----END CERTIFICATE-----
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
   <Configuration>Release</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\hash\sha2sum.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">

 <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid>{8C5CF095-A0A4-54FB-0D48-8DF2B7FE4CA5}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>sha2sum</RootNamespace>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
```

```
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
/>
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <LinkIncremental>true</LinkIncremental>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <LinkIncremental>true</LinkIncremental>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <LinkIncremental>false</LinkIncremental>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <LinkIncremental>false</LinkIncremental>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
```

```
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
     <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
```

```
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
  </Link>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
     <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
-----BEGIN CERTIFICATE-----
MIIDDDCCAfSgAwIBAgIBATANBgkqhkiG9w0BAQsFADAmMSQwIgYDVQQDExtUZXN0
IGludGVybWVkaWF0ZSBtYXhwYXRoIDIwHhcNMDEwMTAxMDAwMDAwWhcNMzAxMjMx
MjM1OTU5WjAeMRwwGgYDVQQDExNUZXN0IGxlYWYgaW52YWxpZCAzMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAw6Vc/T2GYTWj7nGZcy2voZyeWkFyfDIy
oexyJe8eyuWX+YqaSCra1JMcww0Jy8e9/6/aI9ezd1d73eZDcW5h61tagCpBki+W
dYh+FJfCdDdPnSkitWOBLKBK21AQ9dxePvkQBEanDdAk2IwasydCoHEiSCqwXNEz
```

jVJPL38ibbLf9sNO3kk6zOFA3QqVSTJ4BddNh9bHL7y106ekfMhrfyTzSpo3Wj0V
20ThmJZ1NuwYRl3j1XHALP0t8Cp2ZLbXuFsTWqTFNzXj+gWM8b2IfZqmqcew5poZ
4aDkjXXOizRxDPxCHp7rLz9xv1pIIBxady0YWp+w9vxLxFF6rYBLtQIDAQABo00w
SzAJBgNVHRMEAjAAMB0GA1UdDgQWBBQoF/qrn9WnKV3zOnCwMl99Uhmx8DAfBgNV
HSMEGDAWgBTOruRpI5MW/Dw3UCBigw/LdWb//TANBgkqhkiG9w0BAQsFAAOCAQEA
VUnlX//h3T5Ajc85WNkyTuirhSZtIr6+X/AxH4kR/QG5NiaDxP9H0FzMs5FcMni8
3Rs4d2H3CBs+QB7lm/b+xy26vpORwlVFXScHeTEanuXSVsmGPkn7TAQrPoyZgVUN
uy4TGi8Mlkso4gmgehvgTklIV+Emxy32Abd1lRfI8/vOQ1xTdA7f3X98AfWStTya
DGRsQLZE/Q4/Gh57xNqF0ftBIRwt9TbGlu8AyZiIilVECGvE/gtTwuqpQPOhJQmi
NdYTErgD2Wkw9ohifQFo46AMMU1seehtqijW2pC2UjmV5nboPs0eGQmWrfNCjDOr
sZfh98BafcaFGjz605V36g==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDNzCCAh+gAwIBAgIBAjANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTEwMjEyMTQ0NDA2WhcNMjEwMjEyMTQ0NDA2WjA0MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxEjAQBgNVBAMTCWxvY2FsaG9zdDCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBAMFNo93nzR3RBNdJcriZrA545Do8Ss86ExbQWuTN
owCIp+4ea5anUrSQ7y1yej4kmvy2NKwk9XfgJmSMnLAofaHa6ozmyRyWvP7BBFKz
NtSj+uGxdtiQwWG0ZlI2oiZTqqt0Xgd9GYLbKtgfoNkNHC1JZvdbJXNG6AuKT2kM
tQCQ4dqCEGZ9rlQri2V5kaHiYcPNQEkI7mgM8YuG0ka/0LiqEQMef1aoGh5EGA8P
hYvai0Re4hjGYi/HZo36Xdh98yeJKQHFkA4/J/EwyEoO79bex8cna8cFPXrEAjya
HT4P6DSYW8tzS1KW2BGiLICIaTla0w+w3lkvEcf36hIBMJcCAwEAAaNNMEswCQYD
VR0TBAIwADAdBgNVHQ4EFgQUpQXoZLjc32APUBJNYKhkr02LQ5MwHwYDVR0jBBgw
FoAUtFrkpbPe0lL2udWmlQ/rPrzH/f8wDQYJKoZIhvcNAQEFBQADggEBAJxnXClY
oHkbp70cqBrsGXLybA74czbO5RdLEgFs7rHVS9r+c293luS/KdliLScZqAzYVylw
UfRWvKMoWhHYKp3dEIS4xTXk6/5zXxhv9Rw8SGc8qn6vITHk1S1mPevtekgasY5Y
iWQuM3h4YVlRH3HHEMAD1TnAexfXHHDFQGe+Bd1iAbz1/sH9H8l4StwX6egvTK3M
wXRwkKkvjKaEDA9ATbZx0mI8LGsxSuCqe9r9dyjmttd47J1p1Rulz3CLzaRcVIuS
RRQfaD8neM9c1S/iJ/amTVqJxA1KOdOS5780WhPfSArA+g4qAmSjelc3p4wWpha8
zhuYwjVuX6JHG08=
-----END
CERTIFICATE-----
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>

```
    <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
    <Configuration>Release</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
</ItemGroup>
<ItemGroup>
  <ClCompile Include="..\..\programs\pkey\mpi_demo.c" />
</ItemGroup>
<ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">

  <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
</ItemGroup>
<PropertyGroup Label="Globals">
  <ProjectGuid>{A59FAA0B-9C34-1F99-794D-A365A3AA8CCE}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>mpi_demo</RootNamespace>
</PropertyGroup>
<Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
</PropertyGroup>
<Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
<ImportGroup Label="ExtensionSettings">
</ImportGroup>
```

```
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
 />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
    <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
   <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <LinkIncremental>false</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
   <LinkIncremental>false</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <ClCompile>
     <PrecompiledHeader>
     </PrecompiledHeader>
     <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
      <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
     <SubSystem>Console</SubSystem>
     <GenerateDebugInformation>true</GenerateDebugInformation>
     <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
```

2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
<AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
</Link>
<ProjectReference>
<LinkLibraryDependencies>false</LinkLibraryDependencies>
</ProjectReference>
</ItemDefinitionGroup>
<ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
<ClCompile>
<PrecompiledHeader>
</PrecompiledHeader>
<WarningLevel>Level3</WarningLevel>
<Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
<AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
</ClCompile>
<Link>
<SubSystem>Console</SubSystem>
<GenerateDebugInformation>true</GenerateDebugInformation>
<ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
<AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
</Link>
<ProjectReference>
<LinkLibraryDependencies>false</LinkLibraryDependencies>
</ProjectReference>
</ItemDefinitionGroup>
<ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
<ClCompile>
<WarningLevel>Level3</WarningLevel>
<PrecompiledHeader>
</PrecompiledHeader>
<Optimization>MaxSpeed</Optimization>
<FunctionLevelLinking>true</FunctionLevelLinking>
<IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
<AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
</ClCompile>
<Link>
<SubSystem>Console</SubSystem>
<GenerateDebugInformation>true</GenerateDebugInformation>
<EnableCOMDATFolding>true</EnableCOMDATFolding>
<OptimizeReferences>true</OptimizeReferences>
<AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3

```
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
 <Import
 Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
-----BEGIN CERTIFICATE REQUEST-----
MIIBFzCBvwIBADA0MQswCQYDVQQGEwJOTDERMA8GA1UEChMIUG9sYXJTU0wxEjAQ
BgNVBAMTCWxvY2FsaG9zdDBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABDfMVtl2
CR5acj7HWS3/IG7ufPkGkXTQrRS192giWWKSTuUA2CMR/+ov0jRdXRa9iojCa3cN
Vc2KKg76Aci07f+gKTAnBgkqhkiG9w0BCQ4xGjAYMAkGA1UdEwQCMAAwCwYDVR0P
BAQDAgXgMAoGCCqGSM49BAMCA0cAMEQCIGmRFdjjd53oM2Zpt3E5vfqujnA+DHWk
s9OudcSWBdjmAiA7BAYjGnXyL6ATPqM7qnLVGTf3JMT+1rXl7esBm/0APA==
-----END CERTIFICATE REQUEST-----
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
    <Configuration>Debug</Configuration>
    <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
    <Configuration>Debug</Configuration>
    <Platform>x64</Platform>
```

```
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
    <Configuration>Release</Configuration>
    <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
    <Configuration>Release</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
</ItemGroup>
<ItemGroup>
  <ClCompile Include="..\..\programs\hash\md5sum.c" />
</ItemGroup>
<ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">

<Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
</ItemGroup>
<PropertyGroup Label="Globals">
  <ProjectGuid>{80FE1ECF-6992-A275-7973-E2976718D128}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>md5sum</RootNamespace>
</PropertyGroup>
<Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
</PropertyGroup>
```

```
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
 />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
    <LinkIncremental>true</LinkIncremental>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
   <LinkIncremental>true</LinkIncremental>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <LinkIncremental>false</LinkIncremental>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
   <LinkIncremental>false</LinkIncremental>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <ClCompile>
     <PrecompiledHeader>
     </PrecompiledHeader>
     <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
      <SubSystem>Console</SubSystem>
     <GenerateDebugInformation>true</GenerateDebugInformation>
     <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
```

```
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
```

```
cies>
  </Link>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
   <WarningLevel>Level3</WarningLevel>
   <PrecompiledHeader>
   </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
   <FunctionLevelLinking>true</FunctionLevelLinking>
   <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
   <SubSystem>Console</SubSystem>
   <GenerateDebugInformation>true</GenerateDebugInformation>
   <EnableCOMDATFolding>true</EnableCOMDATFolding>
   <OptimizeReferences>true</OptimizeReferences>
   <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
   <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
-----BEGIN CERTIFICATE REQUEST-----
MIICpTCCAY0CAQAwPDELMAkGA1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NMMRow
GAYDVQQDExFQb2xhclNTTCBTZXJ2ZXIgMTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAKkCHz1AatVVU4v9Nu6CZS4VYV6Jv7joRZDb7ogWUtPxQ1BHlhJZ
ZIdr/SvgRvlzvt3PkuGRW+1moG+JKXlFgNCDatVBQ3dfOXwJBEeCsFc5cO2j7BUZ
HqgzCEfBBUKp/UzDtN/dBh9NEFFAZ3MTD0D4bYElXwqxU8YwfhU5rPla7n+SnqYF
W+cTl4W1I5LZ1CQG1QkliXUH3aYajz8JGb6tZSxk65Wb3P5BXhem2mxbacwCuhQs
FiScStzN0PdSZ3PxLaAj/X70McotcMqJCwTbLqZPcG6ezr1YieJTWZ5uWpJl4og/
DJQZo93l6J2VE+0p26twEtxaymsXq1KCVLECAwEAAaAkMCIGCSqGSIb3DQEJDjEV
MBMwEQYJYIZIAYb4QgEBBAQDAgBAMA0GCSqGSIb3DQEBBQUAA4IBAQB95Pkjpg/N
Jbgl5nZcAk8maGMpUFlrhJS4kGutQKZugNX9v8cfABW905IHYXV1dm6zxVcyeqZM
FiOgbV943fu5JbufoazdYXnnR2/iKMigqX4CzZrK3F5ZzegxkfDIfDrn/shC+rWb
SS5WBVLJ3QNj9vwn3/b66IRbp/ViOwHx7+9JT4K/rLId/ynjYf2T57AsmNd/jptc
Zs19fGgtrUXweWkliEZN2zE47Cc53jkx6+Li4TNs4Bjk5P/aXrCP0fBwgGt2K6YW
dQ/nr0PwIbXzVlgUukSTHkJJfhF4Y/WqcUfOPrRdw+zxOLusJ9nzJBR0FOohcBxM
kPBVna0dze/o
-----END CERTIFICATE REQUEST-----
-----BEGIN EC PARAMETERS-----
BggqhkjOPQMBBw==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
```

```
MHcCAQEEIPuPPMxo5e2doI7YfDp60qmEn4YwYs2sb5QlOpFQ3BIJoAoGCCqGSM49
AwEHoUQDQgAEeo5RimyXeYYg8Te/PYJDnMKchyPcEcAqwAwDsDpDHjwT0ZcBnZu5
sO2fxAJrtus0Zv4XMq7ODKpNi2mw4zyPVw==
-----END EC PRIVATE KEY-----
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
   <Configuration>Release</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\x509\cert_app.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">

  <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid>{D4D691D4-137C-CBFA-735B-D46636D7E4D8}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>cert_app</RootNamespace>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
```

```
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
/>
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
```

```
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
   <PrecompiledHeader>
   </PrecompiledHeader>
   <WarningLevel>Level3</WarningLevel>
   <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
    <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
   <SubSystem>Console</SubSystem>
   <GenerateDebugInformation>true</GenerateDebugInformation>
   <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
   <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
   <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
   <PrecompiledHeader>
   </PrecompiledHeader>
   <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
 <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
   <SubSystem>Console</SubSystem>
   <GenerateDebugInformation>true</GenerateDebugInformation>
   <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
   <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
   <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
```

```
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
  </Link>
 </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
 <Import
 Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
```

-----BEGIN RSA PRIVATE KEY-----
MIIJKQIBAAKCAgEA5F2mqEsdntPAEij6HfCYnKiLMGnm6PcfsaFYeFYO1EufOjN5
ZJP90cr3CrCnN9JOAdpBbTpzA0RcIcAdWBzvNNAtIMvSfi22WJYVjzD0Bvs2rCYH
76Yc6vfx7y9zXZcanh8S/2t7B64xmxOWL4RE+f8HWTijAWlyUFDk+DuJWpQK2o0b
hE4S8mX+uUl3afNW5CiPsRky1N1v4a7/J2b7cG+7pDWUcjnvmNCN84v+gSucXfKg
/LiAnZgY7xih2ePEhkkIqn6kU0cVBQj1cZ7hXGRaZ/MnqZ2y+KjiuFot2saNk/v0
vjjW+xOx76qJV99LtN/1qvCYnO1RqMv2EM8WhErLcgiRrihzaz3a2GaumL30CcNi
xrEXRyEjFaO/klqkpuZRHTtyUnkvhUkPUHuHn45XPxZ7a2XRyrSbFyyS0amTjQwQ
CveSRiJFjK5TZ56CVGKF/DmuLSHeTY3vwi+WXVdKMYQ6Zi9jwFJo/S4TRpzp+DTS
H68FrFRqE1+qIVyWQjmhWxuvPhqVkG0IT7CZ0M8lWesysyI759f5D8DhEp/KbWLD
eXWCzcNSbgWGHW5JA+fCV7+8m0PqodIy5D8Lhwm2tI5dA6Qcro8X127RWVaVsN8L
Izdf1THXfnZIm1fDBNUfhXapKfnFV8EvALFX2Gy8M3kZQ3slaGegILfqRKcCAwEA
AQKCAgBg8z1gr1so5b7iNtFQyqcPwyIscJleiCPFdrknhWmQSXaU7+t2frnASkmt
GSg0s6z4bl9ebvULCweOMJCEquwG4OZ3yPBZLzD91OHcQ60mFZq1ZQPzgvM98fud
TujMb+0V+h1HoKq/rP1UV/FnxOC/vbyx7TCO1eR5Io7CsAv1D2q4NDXdaoPyssh8
gysWKP/Xpzyxs//3jPcFuhSK9taCen0QDssx31TP7KKHJgTrc8dTv0EHaZD41uym
/S8hYOg7FmB+eXtr+355/76r+Qa2Aci73ugUw2WK2bA/EdHr0mWi0NGrvFfQiiD9
ncnnK15psLcMVk6EOOB1J/oUUsa8n6/lQiTJYRfFlf0hr+mbMEgdfImM2Xn4wF8Y
Ovapp8Gj/XO7FVVaWW8dIVUrgyrCuOz5SW11Pb0/KFebzOQytST0S3z1j55bUl5L
mDxR0rJU+fMvbdJvMgHgi6YYI1MBbSFmK7/Ue9HZaGxfUPBqXJetOgAJnuoWUqO4
AtpYbLaIiqvdIDi1xF4jDMGIoOl7CnFzU9B3PjCkX4aGdARpXqRABwFT9bpf1lWe
DsEhbIg4/qTWKcA6DxIXaDhgP9eH6NDWS6WKb8L1SZ3mMytjaCxKsV6p7p9DjJR1
dwOmY0Hv7eBYhjVYUj3ybZs6dfFlIg+M5RtarlOsFhZJ9nVhEQKCAQEA/l0FHos6
k5c1726blx7zlRm9mOt+rV1nbEOSZUny++oXGyXrUYvX5NX+p8soF0Im9dCuiguQ
sdKNK6DZCIayennwwEncjKWH+O9VahXxMS9RwtaRDNWJRx3SP6b2s4T1W6PVZdTd
K7MlMB182ckvs67WQ2hMHNcKrTHuTddpAYSD5Lh/QYD6IdWqs6lwLAtmL7/WTkN7
XdPhzVfCXLjeBBqr7PakNM9qI7duw29QpSfnArshDmvwiuVOGVGCcm4qB1RV0sQg
KQJ5nt9X5VoK2SMDR2IzYbq5I/wexiHIbr4kThaGok55lGiCNRjkane+/rSOirZX
Yo0sJ3RTUrBLyQKCAQEA5dXPAYF7lAo3Xpwo0Qou9IFc0qtiFK9pAp0q81DSbDJC
lkZOMm/ofzE6vF6jxja2skXccbEhIDu876m9370uRUAAmfimAdmRhUk+JzrlHXxO
tFSxbyG0iCmwtCSZmiBcMfvFJ/5HepBhxbUDBIc6Pi8EOgjcQdnJYr60KJxbovK0
wr9mnwwaK7SrE+mX5vN2aOwGpG9n61ibUT1aELR9alOZ8H4SlhLtZvgP02YoOCSW
BKKe44fbOk/qUlZG1D6O6/H/OMT4TMyYgaswy0QuMHTjOBXrkAmVSch5dwo0eoxx
dFhn31nF9S5rBZt/PdBPR3imz7U6MoBh6/8olHFk7wKCAQEAxbOTGQxqOPDccP7t
W+YouQjKvqK7URA6JIHYtXVmsLpfvzAX2Mfyw+A4ED7tKDa4hXLvVkhq7GuUYgag
6emXq24/25UNIRw/tRKAtvXbA7mduOyAzRLjoizhj6u8MAf1lIaghIeQaDjTfLRO
qA+hTe1kh/v2vKu/lqIqcMIu0Ykn4owsDMOspsOl7AKUNwedIxvd+/KjXmgjJzFA
1kSx+0qnuoRxWMKl4qDeLHTGn7eF7C96H/VxfuN/clpSI5LQg+Xe1vStcnKECSHa
9V6o8+As2jzPZvR0li2N1b3IRZrwKOmFN337LYiVO6PfVYlBIENCTzoubWEAoqHd
aXWxUQKCAQEAuMDYuLMnbeeQfuM1BGUVPcNHpKnUHCCtX0aMIi+UFxmH4Vj+vxiq
YqRmPMovCMUus7vo6xOiN1EOHfHrChH/QfejBCKW/+GvUt9/sPVs+/jTI675OwZz
IwmwW/8X4oek1SE4aV/EgcfScKWDmX5C2X3d/fDlbaHuewwlsoeOOjy0BeDqU2vd
FckTxNwAGc0YIFurMz/C37LIl9OjtM4CCxjNJD+UHUN1x1IdFqiGKCtw1KUM6IZr
OkLHcAyevzrSlORhb3cWylWlOocsoBlcr+MmTA2C4LRzZ25aBdEUQnbnNMlkJmz5
7o+zxDwtWrk7IY7hORLLh5EgJh9ktX85zQKCAQAZILSp21azS3KzKdAvq5u2KVAV
GumDf1douO5o+5HjV2Kcf5tkzj4A1ffVZKt7auZCNURAG4jaNIccScZBz33EtCuB
wvRQp5f8DN9EQH4yjaNIbPkFrKzgz5AY08n10PBm+X3cY48P27oR/IDfr2wVtCAE
UufjLZCkuUjdCFD1wJSCj7LNwjZURuCTocvtaa7HEqnjW9VB4aAbdtf53WRsbYwt

ZFEWVp8sYc917I6OUJFQcT7jxbv4kbUAXICLaLtaLW2bWfdRtFQSo08pmZAKxxCv
6Vu5VLZ8LGLVkpie8FEaYd/89gEsHh6HgY9LsJN7WxoaJn1sLmEtmyw9xRSW
-----END
RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDCjCCAfKgAwIBAgIBATANBgkqhkiG9w0BAQsFADAWMRQwEgYDVQQDEwtUZXN0
IHJvb3QgMjAeFw0wMTAxMDEwMDAwMDBaFw0zMDEyMzEyMzU5NTlaMCYxJDAiBgNV
BAMTG1Rlc3QgaW50ZXJtZWRpYXRlIG1heHBhdGggMTCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBANJrP7/Y+KjupvlgaOmQYArfGuoh3CzcdPe/mlhq+fxD
8U9qzgSVuVR+FpNZi9DyMljMBrWV1OnZI+cVCDYYkNMa3IkV+AkzJGqwcSBKE+6N
RXZvv+I4xbGymdSSaT6Kh1PgPVk/EYNfLFF30pBsycjM81aMtZgW6aA9xCSp0r8W
XkZodsrJUQerDh/7VmDVEeKanZog8auvrvs/ENiA8d4p/75lOIER4nLz6SSn5Eqy
uXzNCwmT5PVwWStXbDD7EBs3rOtR2VNWQ9o6QdfKQOe/SkIddZr1IWGEJ8JHjtNo
jxcYO67A+Jgp1Jwjk+83eRICs0hlWyeHWfBlbOVIKLcCAwEAAaNTMFEwDwYDVR0T
BAgwBgEBAQIBADAdBgNVHQ4EFgQUyw8Phy/FAvifGQ+G6HWkMiWzyqUwHwYDVR0j
BBgwFoAUlB0h+oI62BWZ0tYA75OwaX8EysAwDQYJKoZIhvcNAQELBQADggEBACFS
6tFy9TpVMUfh1mkr3rFEVtho0NJkRhJW8z2PTmKQa069S9gS+U6+CsqwvM1y3yyh
Pt2q34fhhhbQ+gS8iAm+zvQtBsys3frfVkeKmRzxWDh2LnT+tJi/xtqdlULua5NB
21So46HdlceDTuv2vUbrHgxUS/IEjIL6OZZ0Sc6S6YybvGSioGsRUHO2k2IiOnUa
C+hpBvOkXScnItfdMKAAce71CsZeN97sbxeNIMBDiX9bSy+dZLscEhRwBUABiNr/
sYdYvIpbrFXowjMtBdac+vvhcem7dkCrCdsGylGINWhE2tC9hKmFkFXo4mu/AGDS
M4/59TlMeK8X+WZ9zBs=
-----END
CERTIFICATE-----
-----BEGIN EC PARAMETERS-----
BggqhkjOPQMBBw==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIDQvTm0wfEAKoymv8ePBv7cRxrnM4g6LREnSll5ghQsXoAoGCCqGSM49
AwEHoUQDQgAEFFw4HFFTU/YaL22RORy+q4zm+wuecBLlik4VfwnGeK1q18e1Vx2H
Q/0d2gwOyUr2KZtrE6JOIrG5Q84WTPxgzQ==
-----END EC PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDWzCCAhKgAwIBAgIBGjA+BgkqhkiG9w0BAQowMaANMAsGCWCGSAFlAwQCA6Ea
MBgGCSqGSIb3DQEBCDALBglghkgBZQMEAgOiBAICAL4wOzELMAkGA1UEBhMCTkwx
ETAPBgNVBAoTCFBvbGFyU1NMMRkwFwYDVQQDExBQb2xhclNTTCBUZXN0IENBMB4X
DTE0MDEyMDEzNTgxMloXDTI0MDExODEzNTgxMlowNDELMAkGA1UEBhMCTkwxETAP
BgNVBAoTCFBvbGFyU1NMMRIwEAYDVQQDEwlsb2NhbGhvc3QwgZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBAN0Rip+ZurBoyirqO2ptWZftTslU5A3uzqB9oB6q6A7C
uxNA24oSjokTJKXF9frY9ZDXyMrLxf6THa/aEiNzUnlGGrqgVyt2FjGzqK/nOJsI
i2OZOgol7kXSGFi6uZMa7dRYmmMbN/z3FAifhWVJ81kybdHg6G3eUu1mtKkL2kCV
AgMBAAGjgZIwgY8wCQYDVR0TBAIwADAdBgNVHQ4EFgQU7vPH9R8VpU1HicHTImOy
36fOvVEwYwYDVR0jBFwwWoAUtFrkpbPe0lL2udWmlQ/rPrzH/f+hP6Q9MDsxCzAJ
BgNVBAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEZMBcGA1UEAxMQUG9sYXJTU0wg
VGVzdCBDQYIBADA+BgkqhkiG9w0BAQowMaANMAsGCWCGSAFlAwQCA6EaMBgGCSqG
SIb3DQEBCDALBglghkgBZQMEAgOiBAICAL4DggEBACdVozFq6rUiXo+ib5Y2oPsR
6xxl4Ydn3LpUoYrPpTOrhcXJWW/tOLHGuCF/mSRfUzKaMIfL418cZHYnvumvuttu
6z3tp5E1VsiZCU2MWJnzjKSxFBOss43AmpJHHoapGFZu2pxObBPqegAKHYkKWOLk

```
tJDj47PurWgEek9j1nL7Pc1tVf59fm/ySp4fWkXLLvQiKid1516VioLyacUvK3zU
6Egz8jMt7D5c9KpaExLRTANVsThqO5/dmR36bOwm3Hpbde7DNdgxru41tiLMqJs/
5pX3ceaJ1XQ/l0idj5/9ipvqHHUguyk7H22HwQHQdSD9oIha8kEM3P6CjpfE7yY=
-----END
 CERTIFICATE-----
-----BEGIN PUBLIC KEY-----
MFowFAYHKoZIzj0CAQYJKyQDAwIIAQEHA0IABHaMjK5KvKYwbbDtgbDEpiFcN4Bm
7G1hbBRuE/HH34CblqtpEcJ9igIznwkmhA5VI209HvviZp0JDkxMZg+tqR0=
-----END PUBLIC KEY-----
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
   <Configuration>Release</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\ssl\ssl_server.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">

   <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid>{E08E0065-896A-7487-DEA5-D3B80B71F975}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>ssl_server</RootNamespace>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
```

```
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
 />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
```

```
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
     <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
```

```
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
  </Link>
 </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
 <Import
```

```
 Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgQDA0UszjREl+JklUyevaN8fb0Gp13Dzb4pY3MCoJK15BWoeoUFA
IVvuI0C8bRm/i1OO4BN9tSRrRjW+S89YbYy1C73PUgKZSejjnEFA4chcSOKOhZlM
6K7+Pcrcx+sdiDu1DheODMiSFhoxt+H6IUvBEGkI5AWFu5MDP7wlU/AZfQIDAQAB
AoGAU6o9HEhIuZYuNZDodmdl8YjgECdIfojWmgpnmk4X65xa2KGV45LWBfXMADbC
5mc5QZSfQHuaKuYTKdhRRwh59c9VPwYhN8hdgFzbJS9KfJTDuKhsZrdomHRN2fHK
Jn5MrbVCeZPbYS0M1PzVgEz/BGRp4Ik3RAxTlt+XBtunHA0CQQDz6Gor3gFTdCWM
XtrWEfMW+arWvPUBlOhw3U0YgpWqdea36YeXd9DEIIKn9bQU4g0SjkpO7jd/ccBm
zM89dfjXAkEAymB11gLDd0JZhUCk155uBucaZeez/VNucEgvjWDphRInqJg+2JW2
gSgXNFeSTY9iKlLdBL1zYdywOXM3fd6RywJAIqFYGbxeodO21RROq+BGjHeMWwrf
Godi7Utue9FmoJo21NvyZX4chQw8oM5Q8DocMwtC36wQ8yZac/4WWpqaZwJAbMIy
EXUivrC1k1sOO6I01xjTovhGTlnL/COPCpeOZ6k+DujivVqX3glBjyuQwIXR55To
mmeF3o3PVtCIfehiyQJATsyRPJ1FOYIlIywMSaGHqSpVoebWbDQ6BhYOOvmx5/Zd
Tun1+7WrtPoxM+LQumgPEdx7VDq2L4SetYB/Md1OSQ==
-----END RSA PRIVATE KEY-----
Certificate:
  Data:
      Version: 3 (0x2)
      Serial Number: 0 (0x0)
      Signature Algorithm: sha1WithRSAEncryption
      Issuer: C=NL, O=PolarSSL, CN=PolarSSL Test CA
      Validity
         Not Before: Feb 12 14:44:00 2011 GMT
         Not After : Feb 12 14:44:00 2021 GMT
      Subject: C=NL, O=PolarSSL, CN=PolarSSL Test CA
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
         RSA Public Key: (2048 bit)
            Modulus (2048 bit):
               00:c0:df:37:fc:17:bb:e0:96:9d:3f:86:de:96:32:
               7d:44:a5:16:a0:cd:21:f1:99:d4:ec:ea:cb:7c:18:
               58:08:94:a5:ec:9b:c5:8b:df:1a:1e:99:38:99:87:
               1e:7b:c0:8d:39:df:38:5d:70:78:07:d3:9e:d9:93:
               e8:b9:72:51:c5:ce:a3:30:52:a9:f2:e7:40:70:14:
               cb:44:a2:72:0b:c2:e5:40:f9:3e:e5:a6:0e:b3:f9:
               ec:4a:63:c0:b8:29:00:74:9c:57:3b:a8:a5:04:90:
               71:f1:bd:83:d9:3f:d6:a5:e2:3c:2a:8f:ef:27:60:
                c3:c6:9f:cb:ba:ec:60:7d:b7:e6:84:32:be:4f:fb:
               58:26:22:03:5b:d4:b4:d5:fb:f5:e3:96:2e:70:c0:
               e4:2e:bd:fc:2e:ee:e2:41:55:c0:34:2e:7d:24:72:
               69:cb:47:b1:14:40:83:7d:67:f4:86:f6:31:ab:f1:
               79:a4:b2:b5:2e:12:f9:84:17:f0:62:6f:27:3e:13:
               58:b1:54:0d:21:9a:73:37:a1:30:cf:6f:92:dc:f6:
               e9:fc:ac:db:2e:28:d1:7e:02:4b:23:a0:15:f2:38:
```

```
            65:64:09:ea:0c:6e:8e:1b:17:a0:71:c8:b3:9b:c9:
            ab:e9:c3:f2:cf:87:96:8f:80:02:32:9e:99:58:6f:
            a2:d5
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints:
        CA:TRUE
      X509v3 Subject Key Identifier:
        B4:5A:E4:A5:B3:DE:D2:52:F6:B9:D5:A6:95:0F:EB:3E:BC:C7:FD:FF
      X509v3 Authority Key Identifier:
        keyid:B4:5A:E4:A5:B3:DE:D2:52:F6:B9:D5:A6:95:0F:EB:3E:BC:C7:FD:FF
         DirName:/C=NL/O=PolarSSL/CN=PolarSSL Test CA
        serial:00

  Signature Algorithm: sha1WithRSAEncryption
    b8:fd:54:d8:00:54:90:8b:25:b0:27:dd:95:cd:a2:f7:84:07:
    1d:87:89:4a:c4:78:11:d8:07:b5:d7:22:50:8e:48:eb:62:7a:
    32:89:be:63:47:53:ff:b6:be:f1:2e:8c:54:c0:99:3f:a0:b9:
    37:23:72:5f:0d:46:59:8f:d8:47:cd:97:4c:9f:07:0c:12:62:
    09:3a:24:e4:36:d9:e9:2c:da:38:d0:73:75:61:d7:c1:6c:26:
    8b:9b:e0:d5:dc:67:ed:8c:6b:33:d7:74:22:3c:4c:db:b5:8d:
    2a:ce:2c:0d:08:59:05:09:05:a6:39:9f:b3:67:1b:e2:83:e5:
    e1:8f:53:f6:67:93:c7:f9:6f:76:44:58:12:e8:3a:d4:97:e7:
    e9:c0:3e:a8:7a:72:3d:87:53:1f:e5:2c:84:84:e7:9a:9e:7f:
    66:d9:1f:9b:f5:13:48:b0:4d:14:d1:de:b2:24:d9:78:7d:f5:
    35:cc:58:19:d1:d2:99:ef:4d:73:f8:1f:89:d4:5a:d0:52:ce:
    09:f5:b1:46:51:6a:00:8e:3b:cc:6f:63:01:00:99:ed:9d:a6:
    08:60:cd:32:18:d0:73:e0:58:71:d9:e5:d2:53:d7:8d:d0:ca:
    e9:5d:2a:0a:0d:5d:55:ec:21:50:17:16:e6:06:4a:cd:5e:de:
    f7:e0:e9:54
-----BEGIN CERTIFICATE-----
MIIDhzCCAm+gAwIBAgIBADANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTEwMjEyMTQ0NDAwWhcNMjEwMjEyMTQ0NDAwWjA7MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDA3zf8F7vglp0/ht6WMn1EpRagzSHx
mdTs6st8GFgIlKXsm8WL3xoemTiZhx57wI053zhdcHgH057Zk+i5clHFzqMwUqny
50BwFMtEonILwuVA+T7lpg6z+exKY8C4KQB0nFc7qKUEkHHxvYPZP9al4jwqj+8n
YMPGn8u67GB9t+aEMr5P+1gmIgNb1LTV+/Xjli5wwOQuvfwu7uJBVcA0Ln0kcmnL
R7EUQIN9Z/SG9jGr8XmksrUuEvmEF/Bibyc+E1ixVA0hmnM3oTDPb5Lc9un8rNsu
KNF+AksjoBXyOGVkCeoMbo4bF6BxyLObyavpw/LPh5aPgAIynplYb6LVAgMBAAGj
gZUwgZIwDAYDVR0TBAUwAwEB/zAdBgNVHQ4EFgQUtFrkpbPe0lL2udWmlQ/rPrzH
/f8wYwYDVR0jBFwwWoAUtFrkpbPe0lL2udWmlQ/rPrzH/f+hP6Q9MDsxCzAJBgNV
BAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEZMBcGA1UEAxMQUG9sYXJTU0wgVGVz
dCBDQYIBADANBgkqhkiG9w0BAQUFAAOCAQEAuP1U2ABUkIslsCfdlc2i94QHHYeJ
SsR4EdgHtdciUI5I62J6Mom+Y0dT/7a+8S6MVMCZP6C5NyNyXw1GWY/YR82XTJ8H
DBJiCTok5DbZ6SzaONBzdWHXwWwmi5vg1dxn7YxrM9d0IjxM27WNKs4sDQhZBQkF
pjmfs2cb4oPl4Y9T9meTx/lvdkRYEug61Jfn6cA+qHpyPYdTH+UshITnmp5/Ztkf
```

m/UTSLBNFNHesiTZeH31NcxYGdHSme9Nc/gfidRa0FLOCfWxRlFqAI47zG9jAQCZ
7Z2mCGDNMhjQc+BYcdnl0lPXjdDK6V0qCg1dVewhUBcW5gZKzV7e9+DpVA==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIICUjCCAdegAwIBAgIJAMFD4n5iQ8zoMAoGCCqGSM49BAMCMD4xCzAJBgNVBAYT
Ak5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBF
QyBDQTAeFw0xMzA5MjQxNTQ5NDhaFw0yMzA5MjIxNTQ5NDhaMD4xCzAJBgNVBAYT
Ak5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBF
QyBDQTB2MBAGByqGSM49AgEGBSuBBAAiA2IABMPaKzRBN1gvh1b+/Im6KUNLTuBu
ww5XUzM5WNRStJGVOQsj318XJGJI/BqVKc4sLYfCiFKAr9ZqqyHduNMcbli4yuiy
aY7zQa0pw7RfdadHb9UZKVVpmlM7ILRmFmAzHqOBoDCBnTAdBgNVHQ4EFgQUnW0g
JEkBPyvLeLUZvH4kydv7NnwwbgYDVR0jBGcwZYAUnW0gJEkBPyvLeLUZvH4kydv7
NnyhQqRAMD4xCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UE
AxMTUG9sYXJzc2wgVGVzdCBFQyBDQYIJAMFD4n5iQ8zoMAwGA1UdEwQFMAMBAf8w
CgYIKoZIzj0EAwIDaQAwZgIxAMO0YnNWKJUAfXgSJtJxexn4ipg+kv4znuR50v56
t4d0PCu412mUC6Nnd7izvtE2MgIxAP1nnJQjZ8BWukszFQDG48wxCCyci9qpdSMv
uCjn8pwUOkABXK8Mss90fzCfCEOtIA==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIC6zCCAnKgAwIBAgIBETAKBggqhkjOPQQDAjBLMQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxKTAnBgNVBAMTIFBvbGFyU1NMIFRlc3QgSW50ZXJtZWRp
YXRlIEVDIENBMB4XDTEzMDkyNDE2MTI1NloXDTIzMDkyMjE2MTI1NlowNDELMAkG
A1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NMMRIwEAYDVQQDEwlsb2NhbGhvc3Qw
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDbHH8uC82/ztF1EKCiuM59
quIF4HrYRGOPtb3AsBm5N7gZSg7xXXSAZ0aHBt5bfwYDvcGNXgcV1Fv03OXPPfnB
ESyuarmKvR1nZhfqTr3bFZqCh+TweMOjhYew/Z+pmV/jM+zM6gu1YV7xSX4/oy3q
AQzMQpp2m8TQN9OxFwFhARZZfhwXw1P90XLLTGAV2n3i6q1Q747ii9Rqd1XWcNlr
u/HuOQQ4o73i0eBma+KcR5npKOa2/C7KZ0OE6NWD1p2YawE+gdw8esr585z31igb
J3h8w9DVY6eBNImtJWq98urt+lf85TTGwQ9xLdIIEButREHg/nmgY5OKsV3psO5v
AgMBAAGjgZIwgY8wCQYDVR0TBAIwADAdBgNVHQ4EFgQU4j/mLfTnuKaM3G0XpxhA
J2F2Dx0wYwYDVR0jBFwwWoAUD4m9Y0Hry14XKP9oMD3BiNCcWDmhP6Q9MDsxCzAJ
BgNVBAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEZMBcGA1UEAxMQUG9sYXJTU0wg
VGVzdCBDQYIBDzAKBggqhkjOPQQDAgNnADBkAjBkP1bGlZvxnYySZjdBq4m8lkyz
2cjfqjYs8COEkRkONaVz7888HvFdGpL98uQeFvECMHCyCrHprkGzvq/L9kUnx9Bh
2IHbCzbbi9moYC1XcOxgfsEKmhtVF/uQdf8+3VtGqA==
-----END
CERTIFICATE-----
-----BEGIN EC PARAMETERS-----
BggqhkjOPQMBBw==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIESUhQgXWd8cVQnitNEpOD2JNMqH9ug/wYaY1xW3SaSGoAoGCCqGSM49
AwEHoUQDQgAEgPalqAFB655/t5Mcja4zyZPNlgy4plttUTedbsaaG2nb/GIBhA0X
T/jpPrkakElLAOmV3xd4hq9ho30N8DAx/A==
-----END EC PRIVATE KEY-----

```
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
   <Configuration>Release</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\<PATHNAME>.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">
   <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
   </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid><GUID></ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace><APPNAME></RootNamespace>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
```

```
    <UseDebugLibraries>false</UseDebugLibraries>
   <WholeProgramOptimization>true</WholeProgramOptimization>
   <CharacterSet>Unicode</CharacterSet>
  </PropertyGroup>
  <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
   <UseDebugLibraries>false</UseDebugLibraries>
   <WholeProgramOptimization>true</WholeProgramOptimization>
   <CharacterSet>Unicode</CharacterSet>
   <PlatformToolset>Windows7.1SDK</PlatformToolset>
  </PropertyGroup>
  <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
  <ImportGroup Label="ExtensionSettings">
  </ImportGroup>
  <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
  </ImportGroup>
   <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
  </ImportGroup>
  <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
  </ImportGroup>
  <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
  </ImportGroup>
  <PropertyGroup Label="UserMacros" />
  <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
    <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
  </PropertyGroup>
  <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
   <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
  </PropertyGroup>
  <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <LinkIncremental>false</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
  </PropertyGroup>
  <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
   <LinkIncremental>false</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
  </PropertyGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
```

```
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
     <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
```

```
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
  </Link>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
   <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.targets"
 />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
```

```
    <Configuration>Debug</Configuration>
    <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
    <Configuration>Debug</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
    <Configuration>Release</Configuration>
    <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
    <Configuration>Release</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
</ItemGroup>
<ItemGroup>
  <ClCompile Include="..\..\programs\util\strerror.c" />
</ItemGroup>
<ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">

  <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
</ItemGroup>
<PropertyGroup Label="Globals">
  <ProjectGuid>{23EF735C-CC4C-3EC4-A75E-903DB340F04A}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>strerror</RootNamespace>
</PropertyGroup>
<Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
```

```
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
 />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
   <PrecompiledHeader>
   </PrecompiledHeader>
   <WarningLevel>Level3</WarningLevel>
```

```
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
     <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
   </Link>
   <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
   </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
   <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
   </Link>
   <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
   </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
```

```
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
  </Link>
 </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
 <Import
 Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
AES-GCM NIST Validation (AES-128,128,0,0,128) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"d785dafea3e966731ef6fc6202262584":"":"d91a46205ee
94058b3b8403997592dd2":"":128:"3b92a17c1b9c3578a68cffea5a5b6245":"":0

AES-GCM NIST Validation (AES-128,128,0,0,128) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"aec963833b9098de1ababc853ab74d96":"":"4e0ffd93beff
d732c6f7d6ad606a2d24":"":128:"e9fcedc176dfe587dc61b2011010cdf1":"":0
```

AES-GCM NIST Validation (AES-128,128,0,0,128) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"c4fb9e3393681da9cec5ec96f87c5c31":"":"845e910bc05
5d895879f62101d08b4c7":"":128:"99fb783c497416e4b6e2a5de7c782057":"FAIL":0

AES-GCM NIST Validation (AES-128,128,0,0,120) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"2a930f2e09beceacd9919cb76f2ac8d3":"":"340d9af44f63
70eff534c653033a785a":"":120:"0c1e5e9c8fe5edfd11f114f3503d63":"":0

AES-GCM NIST Validation (AES-128,128,0,0,120)
#1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"fe71177e02073b1c407b5724e2263a5e":"":"83c23d20d2a
9d4b8f92da96587c96b18":"":120:"43b2ca795420f35f6cb39f5dfa47a2":"":0

AES-GCM NIST Validation (AES-128,128,0,0,120) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"b02392fd7f228888c281e59d1eaa15fb":"":"2726344ba89
12c737e195424e1e6679e":"":120:"a10b601ca8053536a2af2cc255d2b6":"":0

AES-GCM NIST Validation (AES-128,128,0,0,112) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"21895cbafc16b7b8bf5867e88e0853d4":"":"f987ce1005d
9bbd31d2452fb80957753":"":112:"952a7e265830d58a6778d68b9450":"":0

AES-GCM NIST Validation (AES-128,128,0,0,112) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"9bb9742bf47f68caf64963d7c10a97b0":"":"34a85669de6
4e1cd44731905fddbcbc5":"":112:"e9b6be928aa77b2de28b480ae74c":"":0

AES-GCM NIST Validation (AES-128,128,0,0,112) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"4e9708e4b37e2e1b5feaf4f5ab54e2a6":"":"1c53a9fdd239
19b036d99560619a9939":"":112:"6611b50d6fbca83047f9f5fe1768":"":0

AES-GCM
NIST Validation (AES-128,128,0,0,104) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"82fede79db25f00be96eb050a22cea87":"":"e9c50b517ab
26c89b83c1f0cac50162c":"":104:"d0c0ce9db60b77b0e31d05e048":"":0

AES-GCM NIST Validation (AES-128,128,0,0,104) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"1d98566fca5201abb12914311a8bd532":"":"590aef4b46a
9023405d075edab7e6849":"":104:"a1cfd1a27b341f49eda2ca8305":"FAIL":0

AES-GCM NIST Validation (AES-128,128,0,0,104) #2

depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"3038771820c2e1319f02a74b8a7a0c08":"":"e556d9f07fb69d7e9a644261c80fac92":"":104:"4d2f005d662b6a8787f231c5e1":"FAIL":0

AES-GCM NIST Validation (AES-128,128,0,0,96) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"0fb7eef50de598d7d8b508d019a30d5a":"":"a2a2617040116c2c7e4236d2d8278213":"":96:"68413c58df7bb5f067197ca0":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,0,0,96) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"8cc58b609204215c8ab4908286e56e5c":"":"fb83ea637279332677b5f68081173e99":"":96:"a2a9160d82739a55d8cd419f":"FAIL":0

AES-GCM NIST Validation (AES-128,128,0,0,96) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"81a5fd184742a478432963f6477e8f92":"":"da297cbb53b11d7c379e0566299b4d5a":"":96:"200bee49466fdda2f21f0062":"FAIL":0

AES-GCM NIST Validation (AES-128,128,0,0,64) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"f604ac66d626959e595cbb7b4128e096":"":"269d2a49d533c6bb38008711f38e0b39":"":64:"468200fa4683e8be":"FAIL":0

AES-GCM NIST Validation (AES-128,128,0,0,64) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"2e308ba7903e925f768c1d00ff3eb623":"":"335acd2aa48a47a37cfe21e491f1b141":"":64:"4872bfd5e2ff55f6":"":0

AES-GCM
NIST Validation (AES-128,128,0,0,64) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"1304e2a5a3520454a5109df61a67da7a":"":"dbe8b452acf4fa1444c3668e9ee72d26":"":64:"83a0d3440200ca95":"FAIL":0

AES-GCM NIST Validation (AES-128,128,0,0,32) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"ecf1ec2c9a8f2e9cc799f9b9fddb3232":"":"ddf0b695aef5df2b594fcaae72b7e41c":"":32:"2819aedf":"":0

AES-GCM NIST Validation (AES-128,128,0,0,32) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"9ab5c8ca905b5fe50461f4a68941144b":"":"96dd3927a96e16123f2e9d6b367d303f":"":32:"6e0c53ef":"":0

AES-GCM NIST Validation (AES-128,128,0,0,32) #2
depends_on:MBEDTLS_AES_C

gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"b5fc7af605721a9cfe61c1ee6a4b3e22":"":"6b757d40558
23d1035d01077666037d6":"":32:"e8c09ddd":"FAIL":0

AES-GCM NIST Validation (AES-128,128,0,1024,128) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"03c0b4a6e508a8490db0d086a82c9db7":"":"ac52f6c1a05
030321fa39f87e89fdb5e":"33316ca79d10a79f4fd038593e8eef09625089dc4e0ffe4bc1f2871554fa6666ab3e7fe7885e
def694b410456f3ec0e513bb25f1b48d95e4820c5972c1aabb25c84c08566002dadc36df334c1ce86847964a122016d3
89ac873bca8c335a7a99bcef91e1b985ae5d488a2d7f78b4bf14e0c2dc715e814f4e24276057cf668172":128:"756292d
8b4653887edef51679b161812":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,0,1024,128) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"b228d3d15219ea9ad5651fce02c8374d":"":"5c7eafaead0
29c3fe3cf3835fe758d0e":"8c35dd805c08686b9b4d460f81b4dcb8c46c6d57842dc3e72ba90952e2bebf17fe7184445b
02f801800a944486d662a127d01d3b7f42679052cdc73ce533129af8d13957415c5495142157d6ce8a68aa977e56f562
fed98e468e42522767656ce50369471060381bb752dd5e77c79677a4cadffa39e518e30a789e793b07ea21":128:"a4dd
e1ab93c84937c3bbc3ad5237818d":"FAIL":0

AES-GCM NIST Validation (AES-128,128,0,1024,128) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"776afcbabedd5577fe660a60f920b536":"":"5bbb7f1b140
84e520408dd87b97705e9":"44631fc9d4a07416b0dfb4e2b42071e3e2be45502c9ddf72b3e61810eeda31a7d685ebb2e
e43a2c06af374569f439ee1668c550067de2dece9ec46ee72b260858d6033f814e85275c5ae669b60803a8c516de32804
fa34d3a213ccfaf6689046e25eeb30b9e1608e689f4d31cc664b83a468a51165f5625f12f098a6bf7ddab2":128:"a5347d
41d93b587240651bcd5230264f":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,0,1024,120) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"20abeafa25fc4ea7d0592cb3e9b4d5fe":"":"3aba79a58c5a
a664856b41d552c7a8d3":"98cfecaae9eb9a7c3b17e6bc5f80d8a4bf7a9f4fa5e01b74cae15ee6af14633205aafe3b28fb7
b7918e12322ea27352056a603746d728a61361134a561619400ff2bf679045bac2e0fbc2c1d41f8faba4b27c7827bceda
4e9bf505df4185515dd3a5e26f7639c8ad5a38bc5906a44be062f02cc53862678ae36fa3de3c02c982":120:"2a67ad147
1a520fe09a304f0975f31":"FAIL":0

AES-GCM NIST Validation (AES-128,128,0,1024,120) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"2bc73fba942ff105823b5dccf6befb1c":"":"902c3e3b69b1
ef8395d7281ff74cce38":"4adec0b4ac00325a860044d9f9519daa4f7c163229a75819b0fd7d8e23319f030e61dfa8eada
bff42ea27bc36bdb6cad249e801ca631b656836448b7172c11126bad2781e6a1aa4f62c4eda53409408b008c057e0b81
215cc13ddabbb8f1915f4bbab854f8b00763a530ad5055d265778cd3080d0bd35b76a329bdd5b5a2d268":120:"ebdd7c
8e87fe733138a433543542d1":"":0

AES-GCM
NIST Validation (AES-128,128,0,1024,120) #2
depends_on:MBEDTLS_AES_C

gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"356a4c245868243d61756cabe86da887":"":"b442f2ec6d45a17144c258fd59fe5b3b":"12cccc3c60474b0a1579c5006c2134850724fa6c9da3a7022d4f65fd238b052bdf34ea34aa7dbadad64996065acee588ab6bd29726d07ed24ffae2d33aadf3e66ebb87f57e689fd85128be1c9e3d8362fad1f8096ee391f75b576fb213d394cef6f091fc5488d9aa152be69475b9167abd6dd4fd93bbbc7b8ca316c952eb19c6":120:"ed26080dcb670590613d97d7c47cf4":"FAIL":0

AES-GCM NIST Validation (AES-128,128,0,1024,112) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"dfa7e93aff73600fc552324253066e2c":"":"c20001e93f1cd05253c277a9445d61e4":"a64d1e20058a1f7e698622a02f7ff8dc11886717ede17bbdc3c4645a66a71d8b04346fb389a251ffb0a7f445a25faf642bb7e4697d2cacf925e78c4be98457996afb25b0516b50f179441d1923312364947f8f1e0f5715b43bd537727bf943d7b4679b0b0b28b94e56e7bbf554d9cf79fcee4387f32bb6f91efdd23620035be6":112:"6ba5e4dace9a54b50b901d9b73ad":"":0

AES-GCM
NIST Validation (AES-128,128,0,1024,112) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"2ecea80b48d2ecd194a7699aa7d8ccfc":"":"8b4db08bafc23b65ae50a2d20661d270":"efc2ca1a3b41b90f8ddf74291d68f072a6e025d0c91c3ce2b133525943c73ebadc71f150be20afeb097442fa51be31a641df65d90ebd81dcbaf32711ed31f5e0271421377ffe14ddafea3ca60a600588d484856a98de73f56a766ae60bae384a4ae01a1a06821cf0c7a6b4ee4c8f413748457b3777283d3310218fb55c107293":112:"246a9d37553088b6411ebb62aa16":"":0

AES-GCM NIST Validation (AES-128,128,0,1024,112) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"d38fee3fd3d6d08224c3c83529a25d08":"":"a942ccb11cf9468186fabfc18c899801":"1c92a4ce0a1dae27e720d6f9b1e460276538de437f3812ab1177cf0273b05908f296f33ba0f4c790abe2ce958b1d92b930a0d81243e6ad09ef86ee8e3270243095096537cb1054fcfcf537d828b65af9b6cf7c50f5b8470f7908f314d0859107eed772ee1732c78e8a2e35b2493f3e8c1e601b08aeab8d9729e0294dca168c62":112:"803a08700ec86fdeb88f7a388921":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,0,1024,104) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"1899b0cbae41d705c6eed3226afb5bc0":"":"82d0910aa53e300a487d880d018d0dea":"6bf5583cc1007d74f3529db63b8d4e085400ccf3725eab8e19cb145f3910c61465a21486740a26f74691866a9f632af9fae81f5f0bffedf0c28a6ce0fd520bb4db04a3cd1a7d29d8801e05e4b9c9374fd89bcb539489c2f7f1f801c253a1cc737408669bcd133b62da357f7399a52179125aa59fae6707d340846886d730a835":104:"c5d58870fee9ce157f5ec1fa8f":"":0

AES-GCM NIST Validation (AES-128,128,0,1024,104) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"8b95323d86d02754f4c2874b42ec6eb0":"":"4f76084acbdef9999c71dcc794238d7c":"ebc75788377c0b264818a6f97c19cf92c29f1c7cdeb6b5f0a92d238fa4614bc35d0cfe4ec9d045cd628ff6262c460679ac15b0c6366d9289bbd217e5012279e0af0fb2cfcbdf51fe16935968cbb727f725fe5bcd4428905849746c8493600ce8b2cfc1b61b04c8b752b915fed611d6b54ef73ec4e3950d6db1807b1ce7ed1dcc":104:"c4724ff1d2c57295eb733e9cad":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,0,1024,104) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"30da555559eb11cf7e0eff9d99e9607d":"":"7799275bf12335f281ec94a870f90a0b":"e735d556e15aec78d9736016c8c99db753ed14d4e4adaaa1dd7eaad702ea5dc337433f8c2b45afdf2f385fdf6c55574425571e079ca759b6235f877ed11618ff212bafd865a22b80b76b3b5cf1acfd24d92fd41607bbb7382f26cd703757088d497b16b32de80e1256c734a9b83356b6fced207177de75458481eaef59a431d7":104:"3c82272130e17c4a0a007a908e":"":0

AES-GCM NIST Validation (AES-128,128,0,1024,96) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"ed2ac74af896c5190c271cfa6af02fd2":"":"e0226e2d8da47badad1fb78b9a797f27":"8f11353ae476ff923013e6e736ffc9d23101a1c471ccc07ad372a8430d6559c376075efce2e318cdf4c9443dbf132e7e6da5524045028c97e904633b44c4d189a4b64237ac7692dd03c0e751ce9f04d0fdbd8a96074cd7dfa2fd441a52328b4ac3974b4902db45663f7b6f24947dba618f8b9769e927faf84c9f49ad8239b9fb":96:"db8af7a0d548fc54d9457c73":"":0

AES-GCM
NIST Validation (AES-128,128,0,1024,96) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"0225b73fe5fbbe52f838d873173959d8":"":"02a048764f48d9aed1147ee922395bbf":"9b46a57b06e156c877e94c089814493ead879397dab3dfcab2db349ef387efcd0cc339a7e79131a2c580188fc7429044a465b8329d74cd8f47272a4ed32582b1c5c7e3d32341ae902ea4923dc33df8062bc24bb51a11d2ecc82f464f615041387f9c82bd2135d4e240fe56fa8a68e6a9a417e6702430a434b14d70cf02db3181":96:"e2c2ce4022c49a95c9ac9026":"FAIL":0

AES-GCM NIST Validation (AES-128,128,0,1024,96) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"89ca3771a0ef3287568b4ac036120198":"":"7e83d2ffa8af8c554cfd71a0db56ef5b":"1bd7a9d6262882bd12c62bd50942965b3cdcadf5e0fab2dc4d0daf0ee4b16e92c6e2464c0caa423cdce88e4d843490609716ec5e44c41672c656ac0e444d3622557ea8420c94deae3ad190ddaf859f6f8c23e4e2e32a46d28df23de4f99bd6c34f69e06eddfdfa5f263dbe8baf9d4296b2c543e4c4847271e7590374edf46234":96:"06b2bf62591dc7ec1b814705":"":0

AES-GCM
NIST Validation (AES-128,128,0,1024,64) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"a41a297bd96e224942998fe2192934a1":"":"6827f2c5a0b7ecd6bbc696abb0adf556":"f32041abd8543415cbac423d945dda5378a16a7e94d9ab5dbd2d32eb1c5048cc7c8e4df3ca84ec725f18c34cfdeaa7595392aabfd66d9e2f37c1165369cd806cd9d2110def6f5fad4345e5a6e2326c9300199438fcc078cd9fcf4d76872cac77fc9a0a8ac7e4d63995078a9addecf798460ff5910861b76c71bccfb6b629d722":64:"49a4917eef61f78e":"FAIL":0

AES-GCM NIST Validation (AES-128,128,0,1024,64) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"a9372c058f42e0a1d019bdb528313919":"":"8d03f423230c8f00a5b6b712d426a2af":"cfef4e70fcc1821eeccf7c7b5eb3c0c3b5f72dc762426e0bd26242f8aa68c5b716ab97eded5e5720caccc1965da603d556d8214d5828f2cf276d95bf552d47313876796221f62ccb818a6d801088755d58cfb751bfe

d0d5a19718d4e0f94b850e0279b3a69295d1837cba958a6cc56e7594080b9e5b954a199fdc9e54ddc8583":64:"b82cd11cd3575c8d":"":0

AES-GCM
NIST Validation (AES-128,128,0,1024,64) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"6302b7338f8fa84195ad9abbacd89b4e":"":"e1bed5c53547cbc85f3411fbb43bb08b":"bcd329c076e8da2797d50dcdcf271cecf3ce12f3c136ed746edc722f907be6133276ee099038fdc5d73eec812739c7489d4bcc275f95451b44890416e3ffe5a1b6fa3986b84eee3adad774c6feaecb1f785053eeda2cfc18953b8547866d98918dbe0a6abc168ac7d77467a367f11c284924d9d186ef64ef0fd54eacd75156d2":64:"5222d092e9e8bd6c":"":0

AES-GCM NIST Validation (AES-128,128,0,1024,32) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"78b5c28d62e4b2097873a1180bd5a3a5":"":"c93902c2819ee494f0fc4b259ee65dd8":"e6b1192674a02083a6cf36d4ba93ba40a5331fadf63fd1eb2efa2ee9c0d8818472aaaf2b4705746011753f30f447c8f58dd34d29606daf57eadc172529837058cb78a378b19da8d63c321f550dfa256b5fd9f30e93d8f377443bfcd125f86a079a1765d2010be73d060f24eebae8d05e644688b2149bc39e18bd527bc066f2ba":32:"eae48137":"":0

AES-GCM
NIST Validation (AES-128,128,0,1024,32) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"3d84130578070e036c9e3df5b5509473":"":"3b9b4950523a19c6866fd2b0cde541fd":"a764931e1b21a140c54a8619aacdb4358834987fb6e263cec525f888f9e9764c165aaa7db74f2c42273f912daeae6d72b232a872ac2c652d7cd3af3a5753f58331c11b6c866475697876dbc4c6ca0e52a00ba015ee3c3b7fb444c6e50a4b4b9bbe135fc0632d32a3f79f333d8f487771ed12522e664b9cf90e66da267f47a74d":32:"79987692":"":0

AES-GCM NIST Validation (AES-128,128,0,1024,32) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"08428605ab4742a3e8a55354d4764620":"":"128f5f4a817e4af04113847a223adeb0":"464b484ed79d93a48e0f804e04df69d7ca10ad04ba7188d69e6549ab50503baaec67e0acba5537d1163c868fd3e350e9d0ae9123046bc76815c201a947aa4a7e4ed239ce889d4ff9c8d043877de06df5fc27cf67442b729b02e9c30287c0821ef9fa15d4cccbc53a95fa9ec3ed432ca960ebbf5a169ccada95a5bf4c7c968830":32:"3eb3e3a2":"":0

AES-GCM
NIST Validation (AES-128,128,1024,0,128) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"0dd358bc3f992f26e81e3a2f3aa2d517":"87cc4fd75788c9d5cc83bae5d764dd249d178ab23224049795d4288b5ed9ea3f317068a39a7574b300c8544226e87b08e008fbe241d094545c211d56ac44437d41491a438272738968c8d371aa7787b5f606c8549a9d868d8a71380e9657d3c0337979feb01de5991fc1470dfc59eb02511efbbff3fcb479a862ba3844a25aaa":"d8c750bb443ee1a169dfe97cfe4d855b":"":128:"a81d13973baa22a751833d7d3f94b3b1":"77949b29f085bb3abb71a5386003811233056d3296eb093370f7777dadd306d93d59dcb9754d3857cf2758091ba661f845ef0582f6ae0e134328106f0d5d16b541cd74fdc756dc7b53f4f8a194daeea9369ebb1630c01ccb307b848e9527da20a39898d748fd59206f0b79d0ed946a8958033a45bd9ae673518b32606748eb65":0

AES-GCM NIST Validation (AES-128,128,1024,0,128) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"43b5f18227e5c74288dbeff03801acd6":"f58d630f10cfca61d4644d4f6505bab629e8e8faf1673e64417f9b79e622966a7011cfb3ff74db5cebf09ad3f41643d4437d213204a6c8397e7d59b8a5b1970aed2b6bb5ea1933c72c351f6ba96c0b0b98188f6e373f5db6c5ebece911ec7a1848abd3ae335515c774e0027dab7d1c07d047d3b8825ff94222dbaf6f9ab597ee":"08ee12246cf7edb81da3d610f3ebd167":"":128:"82d83b2f7da218d1d1441a5b37bcb065":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,1024,0,128) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"9a433c612d7e1bdff881e4d63ba8b141":"ce10758332f423228b5e4ae31efda7677586934a1d8f05d9b7a0dc4e2010ec3eaacb71a527a5fff8e787d75ebd24ad163394c891b33477ed9e2a2d853c364cb1c5d0bc317fcaf4010817dbe5f1fd1037c701b291b3a66b164bc818bf5c00a4c210a1671faa574d74c7f3543f6c09aaf117e12e2eb3dae55edb1cc5b4086b617d":"8b670cf31f470f79a6c0b79e73863ca1":"":128:"8526fd25daf890e79946a205b698f287":"FAIL":0

AES-GCM NIST Validation (AES-128,128,1024,0,120)
#0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"8e9d75c781d63b29f1816859f7a0e0a0":"a9f1883f58e4ef78377992101ab86da0dafcefa827904dd94dff6f6704b1e45517165a34c5555a55b04c6992fb6d0840a71bd262fe59815e5c7b80fe803b47d5ba44982a3f72cb42f591d8b62df38c9f56a5868af8f68242e3a15f97be8ef2399dbace1273f509623b6f9e4d27a97436aebf2d044e75f1c62694db77ceac05de":"748a3b486b62a164cedcf1bab9325add":"":120:"131e0e4ce46d768674a7bcacdcef9c":"FAIL":0

AES-GCM NIST Validation (AES-128,128,1024,0,120) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"fe6b8553002c69396d9976bb48d30779":"786f4801b16de7a4931ab143b269c7acc68f1ed9b17a95e8929ccec7d53413059fd4267bedbf079d9d69e90314c1345bc9cb9132f1af69323157ddf7533ced42b4b7bd39004f14d326f5b03bc19084d231d93bcab328312d99b426c1e86e8e049d380bb492e2e32ad690af4cf86838d89a0dfdcbc30e8c9e9039e423a234e113":"595b17d0d76b83780235f5e0c92bd21f":"":120:"8879de07815a88877b0623de9be411":"b15dc7cd44adcb0783f30f592e5e03ccd47851725af9fe45bfc5b01ae35779b9a8b3f26fec468b188ec3cad40785c608d6bfd867b0ccf07a836ec20d2d9b8451636df153a32b637e7dcdbd606603d9e53f6e4c4cc8396286ce64b0ea638c10e5a567c0bc8e808080b71be51381e051336e60bf1663f6d2d7640a575e0752553b":0

AES-GCM
NIST Validation (AES-128,128,1024,0,120) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"14898c56009b459172fef9c17993b54f":"e7ba6ef722273238b975d551f95d3e77e9b75b24c547b86eafb457d409803bdf6e1443839d8604ee497020e1a3dbd687a819b17fdde0fcf240ce2129792792a58bfcd825773001ee959bf9ec8d228e27ce1cd93d7fb86769a3793361b6f82bf7daf284afc1ece657a1ee6346ea9294880755b9b623563ad2657ba2286488a2ef":"0862f8f87289988711a877d3231d44eb":"":120:"36938974301ae733760f83439437c4":"3fd56897a62743e0ab4a465bcc9777d5fd21ad2c9a59d7e4e1a60feccdc722b9820ec65cb47e1d1160d12ff2ea93abe11bc101b82514ead7d542007fee7b4e2dd6822849cd3e82d761ff7cf5ce4f40ad9fec54050a632a401451b426812cf03c2b16a8667a88bb3f7497e3308a91de6fd646d6a3562c92c24272411229a90802":0

AES-GCM NIST Validation (AES-128,128,1024,0,112)
#0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"fe5253d4b071793b081ebc122cc2a5f8":"b57a0bd7714ae
95e77fa9452e11a7ed4a2bec60f81ad6ddb956d4b1cb5dfc277dcb4034d501801b26733b5e08c710c3cfdccc1b208dc7a
92cd7ebe166320582bcaff64cc943c36fbe7008f004e5db70c40de05fa68b0c9d4c16c8f976130f20702b99674cd2f4c93
aeaeb3abca4b1114dbc3a4b33e1226ad801aa0e21f7cc49b":"49e82d86804e196421ec19ddc8541066":"":112:"e8b8ae
34f842277fe92729e891e3":"c4a31c7ec820469f895d57579f987733337ec6547d78d17c44a18fab91f0322cfe05f23f9a
faf019cf9531dec2d420f3591d334f40d78643fd957b91ab588a7e392447bd702652017ede7fb0d61d444a3b3cc4136e1
d4df13d9532eb71bcf3ff0ae65e847e1c572a2f90632362bc424da2249b36a84be2c2bb216ae7708f745c":0

AES-GCM NIST Validation (AES-128,128,1024,0,112) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"b3502d6f0d172246e16503cdf5793296":"09268b8046f15
58794e35cdc4945b94227a176dd8cb77f92f883542b1c4be698c379541fd1d557c2a07c7206afdd49506d6a1559123de
1783c7a60006df06d87f9119fb105e9b278eb93f81fd316b6fdc38ef702a2b9feaa878a0d1ea999db4c593438f32e0f849
f3adabf277a161afb5c1c3460039156eec78944d5666c2563":"6ce994689ff72f9df62f386a187c1a13":"":112:"21cdf44
ff4993eb54b55d58e5a8f":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,1024,0,112) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"5fb33dd73db309b9dfd3aee605cd94bf":"f4e011f8c99038
c46854b427475f23488077ebf051c4b705a1adfdd493a0a10af7a7e9453965b94f52f61ae62ce9243a82a2dbf9c5a285d
b3fe34ed34ed08b5926f34c48171195f7062d02a6e6e795322a0475017371cb8f645cdcac94afc66dc43e7583bdf1c257
90f4235076a53de6c64f3bc5004e5a9ce4783fbf639fad97":"3f6486f9e9e645292e0e425bac232268":"":112:"7ee5e0e
2082b18d09abf141f902e":"0503cb531f1c967dae24f16dd651d544988a732020134896a0f109222e8639bf29ff69877c
6ef4ac3df1b260842f909384e3d4409b99a47112681c4b17430041ca447a903a6c1b138f0efbb3b850d8290fceac9723a
32edbf8e2d6e8143b1cbc7bf2d28d1b6c7f341a69918758cc82bbab5d898fa0f572d4ceaa11234cb511ec":0

AES-GCM NIST Validation (AES-128,128,1024,0,104)
#0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"a958fe3b520081b638d9e4c7d5da7ac7":"dfa9487378c7d
8af9c8dbd9e533cd81503d9e4e7dab43133bad11fd3050a53a833df9cc3208af1a86110567d311d5fc54b0d627de433c3
81b10e113898203ac5225140f951cdb64c6494592b6453f9b6f952ec5ece732fb46c09a324f26b27cdad63588006bb5c
6c00b9aa10d5d3b2f9eaab69beeddd6f93966654f964260018":"c396109e96afde6f685d3c38aa3c2fae":"":104:"06ca9
1004be43cf46ed4599e23":"FAIL":0

AES-GCM NIST Validation (AES-128,128,1024,0,104) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"ec319fb143eac8215b51541daec268f2":"d298d988e7492
7736237eb8ab09d7a86b854fa2fd1f7f3be83b417ac10aa9291f4af5b3fbaf75a296ac32369ad57ded3984b84711953e47
7de3035ba430a30ffb84c941936e6c8d2cae8d80159876f87dd682747f2dccc36d7c32ab227032b8ac70b313fa4202ea2
36e3ec4d9e4d8b48cf3b90b378edc5b1dbeec929549344f8":"8a4684f42a1775b03806574f401cff78":"":104:"e91acb1
bfda191630b560debc9":"27ce4a622959930f4059f247d29d1438257093cc973bf1bae4e0515da88b9a7e21ec59c7e4d
062035cdf88b91254d856b11c8c1944865fa12922227ded3eecccaa36341ecf5405c708e9ea173f1e6cdf090499d3bb07
9910771080814607a1efe62ec6835dc0333d19dd39dd9ea9f31cd3632128536149a122050bb9365b521d":0

AES-GCM
NIST Validation (AES-128,128,1024,0,104) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"14a3e69f351ac39b4297749a90c1365c":"051224f7b2085
49dcfda5f9d56ce5f0a072ef1f23f3810c693516c92622be6ed4d7a9e0f9450980ba490b2e9e3468ea7eef10bc9ebd673d
91f32b748c1bf2c50cc4ebb59fc409c6d780bba00700d563ce1dc9927a6c860095a42ed053f3d640debfbfa7a4e6d5de2
34af19755000d95e7f414f1f78285ee165410c020038286b":"eb1c6c04437aa5a32bcc208bb3c01724":"":104:"e41881
5960559aefee8e0c3831":"797310a6ed9ce47cdc25f7f88f5dbbf6f8f4837701704d7afced250585922744598d6f95ba2e
ecf86e030cc5ee71b328fc1c4f2d4df945d1b91a2803d6ae8eba6881be5fe0f298dd0c0279e12720ede60b9e857ccca5ab
e9b4d7ee7f25108beebbfe33f05c0d9903bf613c2e7ed6a87b71b5e386d81b3ae53efd01055bbcccc2":0

AES-GCM NIST Validation (AES-128,128,1024,0,96)
#0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"c34827771fc3918d1cee09ba9401b832":"ce79701b66106
6e53191c9acdaf677ad41622314898d7216e3f113e2e6e215d26d8bd139827f06ab3ea5c4105694e87db1dd6cec10e1f8
6a8744d4c541f08e40319e22ab42fc1a6c89edfd486b6f142c6bbbf84a73912e0b2e55b79db306ccabf839855afdd889e
52ae981520c89e7dc29bb2adb1906cca8c93fcb21290a095b":"2379bbd39a1c22bc93b9b9cc45f3840b":"":96:"26e1f6
cf0d9e0f36dfd669eb":"FAIL":0

AES-GCM NIST Validation (AES-128,128,1024,0,96) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"b1f9bd2006ec550b7b9913d383200b5d":"6d9fc8f586d50
d6e0128172ae147844e80136905d3a297497a9566ca7c7445029028f14c9950acee92a5c12a9150f5e024e01c7505dd8
3937542b0b1288de9c292ae8ad918a09b2edf8493540b74c73d2794f2eb6eed18eba520ddea9567462c83330f33d7892
fcde0b10c73a4e26ab1bef037cec7e0190b95188e9a752fee6f":"ca28fa6b64bb3b32ef7d211f1c8be759":"":96:"c87aac
7ad0e85dbb103c0733":"FAIL":0

AES-GCM NIST Validation (AES-128,128,1024,0,96) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"8b2cef1a92aa0af2b00fb2a99855d5bc":"fd09525ef3c65a
b5823e1b6c36b4a9449a3975c5d3a9e7e33c61fb32edcbb8e8c915b6202e3fbce87d73cc3b66d83d9ea7e1e353cc7468f
08626932cf0235563e2a28953ee5a0afadb1c3cb513b1f1fc9a8a6cf326174b877448672f7731dd6430a51619da1a169a
b302da5af5b38802f8bbf5890b5d9b45deda799679501dc4":"08d87b7acee87d884667f6b1e32e34d0":"":96:"3bd7685
318010b0c5fe3308b":"583e64631c218549923e8ad33b728d07f23b0f19d2aff1ad7e20d564c591db0e117caa8f21e3f3
345e3d84f0ccbb27274cddf9274410fc342cb2a5d4aea4e925d0dd5350389ee0dea23a842ff3f5c1198374a96f41e055f9
99cfbc2f47ceaa883da8eb6ff729f583eff1f91bd3f3254d4e81e60d9993b3455e67f405708e4422":0

AES-GCM
NIST Validation (AES-128,128,1024,0,64) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"175c306f8644b0c4b894ae3d0971505e":"fbe7ced7048f8
3e3a075661c4924eb77da1b4d6019d504afb942d728b31fd3b17557bd101c08453540a5e28d3505aeb8801a448afac2d
9f68d20c0a31c7ef22bd95438851789eef1bebe8d96ac29607025b7e1366fecd3690ba90c315528dc435d9a786d36a16
808d4b3e2c7c5175a1279792f1daccf51b2f91ac839465bb89a":"9860268ca2e10974f3726a0e5b9b310f":"":64:"f8091
05e5fc5b13c":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,1024,0,64) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"08c0edcfe342a676ccdc04bdf854b4b0":"1fc8ef8480c32d908b4bcbfa7074a38e915c20ed7a1c608422087e89442d7c5af6fe9c9a716c55793248062d8e6c6e8e904e2804da3a43701e4c78ecdb67e0b25308afc6d9b463356439cd095cff1bdf0fd91ab301c79fd257046cba79a5d5cd99f2502ad968420e4d499110106072dc687f434db0955c756a174a9024373c48":"4a7b70753930fe659f8cc38e5833f0c7":"":64:"9ab1e2f3c4606376":"983458c3f198bc685d98cea2b23cf71f0eb126e90937cab3492a46d9dc85d76bbb8035c6e209c34b2a7187df007faabe9f3064dc63f1cb15bf5a10655e39b94732e0c6583d56327e9701344e048887a81b256181cdfa9ec42ebc990875e4852240ddcb3cbc4ea4e6307075fd314f7190f3553267bd68b19e954e310ec3f8dbab":0

AES-GCM NIST Validation (AES-128,128,1024,0,64) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"241067a0301edf0f825d793e03383ea1":"6984bb9830843529fad7f5e7760db89c778d62c764fcd2136ffb35d7d869f62f61d7fef64f65b7136398c1b5a792844528a18a13fba40b186ae08d1153b538007fc460684e2add8a9ed8dd82acbb8d357240daaa0c4deb979e54715545db03fe22e6d3906e89bdc81d535dae53075a58f65099434bfeed943dbc6024a92aa06a":"a30994261f48a66bb6c1fc3d69659228":"":64:"36c3b4a732ba75ae":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,1024,0,32) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"03cccb5357bd2848332d1696f2ff90cb":"5e2f18cbc1e773df9f28be08abb3d0b64d545c870c5778ac8bb396bef857d2ac1342ae1afb3bf5d64e667bf837458415d48396204fe560e3b635eb10e560e437f2d0396952998fd36e116cd047c1d7f6fc9901094454d24165c557a8816e0d0a8e0ce41e040ba6f26ca567c74fc47d9738b8cd8dae5dfc831c65bc1ba9603a07":"e0754022dfb1f813ccaf321558790806":"":32:"c75f0246":"FAIL":0

AES-GCM NIST Validation (AES-128,128,1024,0,32) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"4e5e53c84a05d5a5348bac7b2611cf62":"489c00c05dec06f282924c680f621ab99ac87f7d33ebbb4ca0eee187ec177d30d2b4afb4ee9f0dc019cf1a4da16d84b7f5f5c7fce72a32461db115b5a5a433024fd5ed3d47161836bb057a0189ed768f95e45fa967d0cc512fc91b555808c4033c945e8f2f7d36428dcb61f697e791b74e5c79b2bcb9cb81bec70d8119cd8d76":"47e40543b7d16bc9122c40b106d31d43":"":32:"81eec75d":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,1024,0,32) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"2c94008bf377f90b7a1c0d2ea38f730c":"7b3d619d115de9970b2df4e1f25194940b3f3da04c653231e8e6946de9dc08ae5ba37e2a93c232e1f9445f31c01333045f22bd832e3b5f9833f37070fafb0ef1c44cc5637058ab64d9e07bb81b32852d4cf749a3ddbfdb494f8de8bb4e31f46033f8a16bc22e2595d023845505ea5db74dd69ab4ca940078b09efb4ff19bdb66":"abfe92931a8411a39986b74560a38211":"":32:"47d42e78":"FAIL":0

AES-GCM NIST Validation (AES-128,128,1024,1024,128) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"69eedf3777e594c30e94e9c5e2bce467":"5114e9983c96fe

cec3f7304ca42f52aa16cb7c6aadfb62ad537c93a3188835ca0703dad34c73cf96435b668b68a7a1d056931959316e8d3
ab956bf64c4e07479c7767f9d488b0c0c351333ccf400b7e0be19a0fd173e3f2a1ae313f27e516952260fd2da9ab9daca4
78ebb93cd07d0b7503b32364d8e308d904d966c58f226bb":"a3330638a809ba358d6c098e4342b81e":"df4e3f2b47cf
0e8590228fcf9913fb8a5eb9751bba318fd2d57be68c7e788e04fabf303699b99f26313d1c4956105cd2817aad21b91c2
8f3b9251e9c0b354490fa5abfcea0065aa3cc9b96772eb8af06a1a9054bf12d3ae698dfb01a13f989f8b8a4bb61686cf3a
df58f05873a24d403a62a092290c2481e4159588fea6b9a09":128:"5de3068e1e20eed469265000077b1db9":"208e632
1238bf5c6e2ef55a4b8f531cbbfb0d77374fe32df6dd663486cf79beeed39bb6910c3c78dd0cc30707a0a12b226b2d060
24db25dcd8a4e620f009cafa5242121e864c7f3f4360aaf1e9d4e548d99615156f156008418c1c41ff2bbc007cecf8f209c
73203e6df89b32871de637b3d6af2e277d146ae03f3404d387b77":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,128) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"45cc35311eedf0ba093bf901931a7036":"5dc8d7525eaad
035c19714ae1b1e538cb66a4089027245351e0ad9297410fb3a0c1155407c10a8bb95a9ca624a9c9925dac003ee78926
c6e90ff4ccdba10e8a78bda1c4478162a0e302de5ff05fb0f94c89c3c7429fb94828bdcd97d21333c2ee72963ee6f056ce
272b8bab007e653a42b01d1d2041ba627f169c8c0d32e6dae":"fed5084de3c348f5a0adf4c2fd4e848a":"6e210914e4ae
d188d576f5ad7fc7e4cf7dd8d82f34ea3bcbdb7267cfd9045f806978dbff3460c4e8ff8c4edb6ad2edba405a8d915729d8
9aab2116b36a70b54f5920a97f5a571977e0329eda6c696749be940eabfc6d8b0bbd6fbdb87657b3a7695da9f5d3a7384
257f20e0becd8512d3705cc246ee6ca1e610921cf92603d79":128:"266a895fc21da5176b44b446d7d1921d":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,128) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"9edb5231ca4a136b4df4ae22b8588f9f":"493df801c57f8b
b591955712d92d3fc34518f0599fec8533b2b4473364e1df4f560c12444cf50eeb584676b7e955c742189de6b50b8e01
2dfa6642f3679fb02bc6d8e08d1db88c8ae955a7946263e06494e17f8df246b672942661e5563302252208f2e00a0d77
068a020e26082c291a75a06f63c41e2830292a418b2b5fd9dd":"c342e9bdabe7be922b2695f5894e032c":"a45c7f8032
ac5144deef8d5380f033aea2786b0592720a867f4831eaccc6b85d3fd568aedc6e472e017455b0b5b30cf7a08ea43ca58
7f35e1646ecd9b4dc774d11e350c82c65692be1e9541cbd72a283bdcf93dc7115545f373747b4f8d5915ed0c42fbeefd3
e9bd86003d65efc2361fde5b874ddabcf8265e6b884615102eff":128:"5ed3ea75c8172fa0e8755fef7b4c90f1":"56696e
501fac1e8d5b83ef911ed11337d5d51ff5342a82993dd5340bb9632e6606eef68ec5fe8cec6b34ebbc596c279e6cbc922
1c4cde933f6d93ae014e3c4ca49593f35eaa638606d059519bac3a3373519e6184e7227d2aa62170c36479fe239cb698b
fca863925a4c9fb1338685a55a6dfd3bd9c52d8ae12be8551fce6e1a":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,120) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"d5fdcb8f5225090e63fae9b68f92c7cb":"d39b9cba95e3a3
aab9bc1d03ff475c04faeb5b7f0510777f39e5a05756606eb7ddd154aac035d9ddaf3535629821dd8f014dedd52cd184f
52fc706e3c89a3a271398c9125d9a624dafb297a56022ca2ea331ea7359ab5e65f8e14814788e64e0a886a9b1a0144bf2
68fdcf9d94c3d10a0452f40111da9df108252e9039eacea3":"581c818282a0905df5ffff652e5604e9":"f1ae6cd7b07f26
1105f555cf812a1d5bf8dd9aac07666318acffa11abb77d0238156663acbf7543825b45c6e9cddb481a40995ecd78bb5f
4cba5df7c7efb00fc19c7f45e94d37697aca8ef368b99165393b6107f900194c797cd3289cb097eb5915f2abfd6aa52dd1
effffdde448e30075a1c053246db54b0ec16eadca1c0071":120:"827e66b5b70dce56215cfb86c9a642":"cec11a12e47fd
443f878e8e9fe23c65f29dd2d53cec59b799bcb0928de8e2f92fe85c27cec5c842ef30967b919accafe0c0d731b57f0bb5
685d90a3061cb473e50e8aeca1346d1f47f7db06941f83f21ba5976d97c28cab547d8c1f38387a04b8a0b212da55b75fb
af9562eeeabd78eadcbab66457f0cd4e0d28133a64cb063f":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,120) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"036198cd3a3ab9319684d0f811cf2992":"6b95b9e82a695fb7b466ce3adb536f525d8314f95eada39efb49baf121093ce7d5439f0d8223e03530b85accd388a70650ca9f7e63eb32afecb7b1916ed9b762128cc641caf3e08e027c3d88481d653b6b15172e977dfb9b3f88465911aee162501cbf8501ce2b66ee151bbfdc23225f638f18750c239d62471663e5ee2a5856":"47dffc6b3b80ffef4b943bde87b9cf3c":"ec4de476cd337f564a3facb544d0ff31cd89af4c3d9a28543e45156189f8eff8f804494dda83a1fb2c30ce858884a01ec63db59268452b1eea0f0d48280bb7340eaacc84509469dd94d303774d053d7ab4fb5f6c26581efeb19165f8cb09d58ec314d09ab8356731e87fd081f661e7b2d1a7c3aa4af5448a12b742e7b210b0b0":120:"6cf68a374bea08a977ec8a04b92e8b":"5c2f7c408167be3d266ff634e1993fe291aef7efae245fa0b6b5bde886a810c866ae6a078286684d1b66116e636e285f03646e09f3c4ed7b184e7c171ba84f3bfd9500c6f35964a404892b4cdcdd3f697fc5b01934a86019810987a9fea7efca016049873f1072f62df3c17f57ea1d88ccd8757f7e3c5d96e8a18d5366a39ea9":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,120) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"c9fbbff8f25f951ba874dfc5ff38584e":"ca401071396da00376add467490abc6e6a7d8a85852026979f7013a09cf689113c8d833560cd6c5b8fdaa8fdd818e773ac13954839a0a2c91efeaf4e0e14de43308419a8b86fa2ae600a88a6bd39dfaabc16a3c7c1b77a5c2aab7f7caceb2f8595324125efbb7c96ba16c47d0bd10568b24bf445d72d683268466e68e46df500":"1c1fc752673be6d4ff4cc749fc11e0fe":"abfde0b60acfe265b62ed68ebebc1f5f725f155c4b8a8aeec8d704701c51ff7817060c1b0ce6b80d6efc9836c9ea2bc022ec67db4cd34e945e3a1b153fd2e0f7ac84bb4b07e04cbb529ee24014b16067f9f082b940c9d5e54024d3e5e9103104574785607215 87da7b5343d89eec5a8fce389c01185db15e7faa9a3fa32e8ab9":120:"ff0b2c384e03b50e7e829c7a9f95aa":"239637fac6e180e71b2c9fa63ce8805f453d81499623ec2deba9b033350250662897867bffaf0c314244baf9e1fe3e1bb7c626d616bfbf3e0ac09a32aaf718b432337c9dc57c2d6fc4a0a09bdc05b9184d1b90c7193b7869f91e2caa8b3b35c10c6621ffae4c609bdf4e4e3f06e930541c381451ef58f4f30a559d2b79b0e6b6":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,112) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"3a314ec178da96311e42334a616fb38b":"518b3f5384ab54f80497d55be7a5d6902bc7718386212c2ec7537db331514b3838f104bf9054e03039a4cfb73f41e5d0a9648e569ed738cea8d33917430dff6afa8f07a75e324b9262fa196a4439dcd66b0535ee5bea0d292600227c2a79ed03be0671740e5cb7b306d855612bd3abcbf02cf7e7cecbb6cdbb33d57b4e3234a2":"d7ea27c819e3eb2666611bb1c7fc068d":"db8dcc31a5681f13d56abd51bd2dcb0d2b171628186e215a68bf16167b4acd00c3441973c3fa62fa2698ee5c6749fc20e542364d63c40756d8bcff780269e5201bafdced3cdc97931d8203873431882c84522c151b775285d0a3c5d7667254c74724ff0ea9d417aa6c62835865dfded34edd331c0c235a089427672c5a9211c9":112:"1e774647b1ca406e0ed7141a8e1e":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,112) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"e818372a63b7e2c23b524e29ba752bdb":"c1bf1b702a95ceaa6b48a1cdd888ae51f58a9fc3232bd6c784529a83301c6d0cdda6e605ad9a2563f54a8d59f624ae7c589e48b85041a010dcb6fb8739d43e79a456fc0e8574af086df78680460c3cdc4e00dc3b9d4e76b0de26e9aec546705249fa7e7466c01001c2667eaf2813be1f0f116916f34843a06b201d653aa1b27e":"36e617e787cb25e154f73af1da68cb06":"71801d69796c2ce36b043c157aec9fd2e06fd1ec596126d10c26b6d44e3dc36c4fa30a030d65c382b6ddfd958e71fe9c16732e595137a

3d6764c15480fc3358e9a113ba492b31274663f5842df5d1cc6bad70e83b34675a4411e2e70755aede0ff5035601be130562e27a20283d6f144ff1bdb5276dec05fad80d51b28d50688":112:"3744262bc76f283964c1c15dc069":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,112) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"9a04f16882ff45816739d1b6697ce8b7":"6a4f3dbb3371f64258fd1f831349e745a4e19a33aad794b1de3788729618beed619586092120e9e5dc3ac6e0d52f991f7be61afbfaa4399ac716ad79a2734827254b1627791dc92a128a6f43426b8085dee94242e83176a3d762658f18ecc1e37e3e1531648c9ced212ea2cf3b3843cb92cb07730f30fe2dca3925470fadd06":"66f504d9a9128ad7fb7f1430d37c4784":"f641c53c83c4fb1ff8044bfa97cdf63fe75d8159d65b3e5ad585b89c083a53cf4a2f7a58eaeaf45fa71f2c07bc5725a6b03307d7f32884a133a4c803700bf1e12564b98b71f63b434ddf13ad2c467dda25ffa6effcafa72452b20c34cfae71e47096f8745b487e9f1945f5bec83f7ec2709a13b504d92315b1b727a78902be84":112:"fbb37084396394fecd9581741f3c":"FAIL":0

AES-GCM NIST Validation (AES-128,128,1024,1024,104) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"38cf029a4b20607030586cd2d82146e6":"f4c9f4476561c9ebdac71b282ae6e2f9f03547da98e66d4d857720db2fcc9ed1f363858db34c9dcaca0109d7c81db24150493115f2bb6985efa8686e3d2ab719d33b230aa4c5c70696bf42f225fb3c6704711c054a882d89b320884a78cb59cd2100496edf4010487597fb9135d8ca79693a43843e9626fd6c64a8722b3a27dc":"6330084319e2bf32cd5240f4826944bc":"80746cfb0127c592f8164d751b0e14a5b379056a884cece7ee4e9b80538d7ff6be56a3b19c135786722aaf315123b47672b0251e87ea45f0fd3601cf93f9efa6cbd9ad537f54d57f1e187f821faac24096ecec19d137c9f4cf145c278af4cd8de01c7758784fda06f1cc62d92ae1977786f3d0645714ab4ab6f48c8794b12f73":104:"7b021de5cda915ba58f90ceef4":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,104) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"cf4d81fc5997c744a572bed71f4ae609":"f3d65d70326e641fbe7fd945fe9cf66c74f17d0d1020ae8ac488f39b7285c99d8632bc2201960f3d77daccfecc04428abe0853aa8d82b90a93127c72b2d2af53f7f1bd0afb99d50f0b3b24e934ec98eddb278b2c65866442cebf10208c7ce1b7ecf764858480b2a269b106fa6d2428d5ad17612e53e62ccc7ad1184663aeb9a7":"bc4e20c56931c967ce8e3b8f5f1c392f":"b6b8294abf7da5703f864721f7904d3821f5568bf4b269e44edef4f1c95ddc172d83a06c0ad9f7f1fd2e292c17a876392bc5bb705d370b2f16ff721bef7648f423346fd3a4d762676e6fcf2d690553a47224af29afed0f452d263be90eb8150a13d720f1db6f1abc1c2ec18cfbf93b8ed3c5aa7cfc1dcb514d69f90409687a4d":104:"0a86142a0af81c8df64ba689f4":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,104) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"d88ad40b42ead744f1b7a36685658be1":"e99d2566fe6bcb2a04d167605db7c0f1e5567ff2d8d3292c15bbccc5d1e872bcb15a30b3bb8b1eb45e02fba15946e6bca310583a6740845a0f74f4ebfd5c59ced46875823e369e0447cc3e5d03dae530adf3c9846362c94e7f9d17207bf92d4d59981d8fd904eb8b96a0a23eb0f8d7e7a87e8e8892a2451524da6841ce575c27":"52c3158f5bd65a0a7ce1c5b57b9b295e":"dde2663335c40e5550ae192b843fa9fb4ef357b5c09d9f39dafda3296a4d14031817ee4dc1a201d677597d81e37050cd3dc86c25adbd551e947a080b6c47ec7be8a927ef7920bd1bb81f2c59801a2b9d745d33344cbe4838bcf2eb8dce53ab82c75c9bbab8e406597f6908aaa81fbbdef25aa69116c8f7a8cdc9958435aa32ac":104:"7643b3534eb5cb38331ed2e572":"6f87f6be2f4e7421aa26fe321045d1e23066a02158634bef35890581c92367d0bc232940de30974c70a66c60137a9f3924d12db1e5bc1b0e7131ea3620a25eb805b7d670263b82c8bbfcd6839305025390fc17d42d82daebe1b24f73ff9aa4617e3866785dded88f8b55ef89b2798ea2641a592a46428d9020f9bf853c194576":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,96) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"c3ce86a212a30e724b4c624057db4e79":"3582ef7a9565c
9a8e4496750ee5ca3e3a80df6238f7b7608e3394ec56d1360777921da039ede34abcedd01081babd496ba4de74a7de50
1181d6bb2022a6cc7f79d89a4c6a97676fb0f2b42f70e2d0bc1eaac364c3646df4f611c1d6b09737451b81b5a4da73c05
fb58391c74e44498b80b26f1c29562d23c39b5d3f086b280cb":"9e03f0dd4cb2b3d830a6925e4400ed89":"92c48a39d
93ea3308f55f6650d33fdf17a902076d582a94a82ac99496de9f62312292b844bbca5a683ef0f0710bbc1c7f89cbcca8f9
c0299f154590d32059bd99fca5d78c450ede0d11d55075947caf2151218ce7a06c1e81985a7781a3444054170b457fd7
ba816026310112abb47c8eddfd3ab7f679a0f60efc6c6dd3b759e":96:"3230fe94b6ccd63e605f87d0":"052347a4273cd
dba65b2a0b961477f07edee440a9117ab204359d2dd45ad2a6dad3b60ead891e7da6d79f3017ac90f95725a0089f04d2
5ce537bf53b7ea8e1ea58692d34c221db141e2a9fd7211adcee03ef8b5bf3c5d36311d20bb3d81f70f7e7272d0e2b6d12
293b1a2c31b70f140a8f08d98c6231a3c429c3d0a10b2e1c1c":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,96) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"a0155360b84420b5bf4fb410ea02f31e":"ecdb51522fc440
f7471ea6a31f7c1ef1ec2153e5bcf6303297dbf8ddb3830b45ed9866157375ce4bdeb5e32fcbc6607984fccd7e65526287
36608ab13072856d432ceccd3e90d1bb52ca9ada9cee90eb89ac10e887a1978fd0fb3d7bb20caaf35539e150be8044b72
5b8427c4c4a910f79980865d36344a8784bcc3d58460acb":"46f0386be7363887e7e357376305eab5":"611bc290f917
98ad84f0a5ecb5a7cb8fa35e9ab6a5a51c9869a68a076e96f92c9c117595f92cbac5d33343fa2accd2541473907cbc5479
2c5e215ae857424c921b04ca4b81376bbedbfcc0e565c118f2aced08f247698eed5e2d202c48245161cabeac9fa195219f
9799fa253e339561e13012167f1d02b4012b7791b7c863ba":96:"ac5addcc10cae6c1345520f1":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,96) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"694f621f594d96b16c32254ff06f3f9c":"e61476b8b7f101
ca6005f25af2b9bee795d62720bbbf59357057ca7cd473e00f0d465255fce8d6164657603323549fb4e3d33fa51054b1a
70cc7e492916dea85453e9107fe781bfeb4a622c5b2306a8dddef99386dc50745003aa7220cd7f32fb0a060fa76825767
69a48f9169c7d11fe0a8a61b95f5d6dfcf216f7d0c652a84":"542db4e107485a3cd24c7ad337a4f1b5":"27b7bfa5eb34b
a376e515e58ab8b6556c396820d0074a1fe3b984945dcf5251ca450456ccb4bb66ec739b03fdc5f72d24553e843255ad
c012d1f1c95aa3cdac5d12926465354217203052cbd4869a8b5be2e01d0fe66b5a6a8da0a2ce351557e2991ce77baa81
2b9c67b8e1c5a1fc348710e1a73a0fd49acfd538b7db6bef8b3":96:"0bdef4d771a1740381e7db97":"8b27a338fd2153d
304f04655e09bd9bdf4468890ecce1e3b51de2c9a25a8d9336a9acd753ce270b1fe8d50196feac68145e0fd59c9cb3aa7c
1e8af03494bc4279c6e287c849f3c775ada584ae173100946ae6921ef7c96bbc6f216093548702cf1867bb1bf1f4c9e90a
34230a2b2aeb584622dd615023a43a406e64428bd9170":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,64) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"78826a5215a1d5e1b39cad5a06861f8f":"0fe2c798d7015
d3e2f8725648d95729c45d357dc0c89fc63b9df5a68d3e65419540f663e9190793a29c58c495d5c6a731782acf119e2df
8a96fb180ad772c301d098dbc5e3560ac45b6631a01cef7eed6db51f223775d601d2e11b9baa55e2f0651344777e5a03f
6738a2013626a891b5f134f07b16598b8cbe3aeaefa1c2a26":"feb9d740fd1e221e328b5ef5ed19eff5":"ca9411b368d82
95210d7a04da05a351d287f2f67d978ef1bb936de9f8065473f6fa11495da2eab13a1002231c86411d5409bbc718e2042

ee99e013b1df1ef786e9fc1f2d43293c854128184efb9317c4ef82a002eac8b28fcd91d8a714a3aa25fc3c0ae4af9f4bcf5a
d19a30cd8ec4b1785df70aa92074da419abe433dd4c435":64:"a724bbb295a02883":"FAIL":0

AES-GCM NIST Validation (AES-128,128,1024,1024,64)
#1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"d450f5253251121606e56687952bf2f1":"479b4f421bd8a
c7f615c4a507da187cb5d4b1f1e2c6113d1f9678c1ba92dc5e17c5b525d7f3208733223eb82af0820b8476e9b08ca714c
e044417b24d2238720cb8ffdc69db558cbaff52e3651b400e16c9d5ac8ed8949a19c35516f80394a04bd1cfdced7b204f
779d792086e00b2ebca2f55a1140e85f5ee9ac7cfc5a31747":"fe7ff90b020fc77d7fcd90bc583850ac":"a3bca9ff25a600
06eb18f993dcdc99681e414e27605264dfd25652195d7fe1489550afd07fc7346b88d93b59eb6642913646e93bf50ee1
db5dd30106cf181124d8ad01c72ed99038c9798620abdf5c78c419b08c97f982b34d9e9105d9aa4538afcd37f62e2412f
14f7a248fcd60abaf2b66cd4554767f99030f1a495d56a5ae":64:"6446398aff73ed23":"FAIL":0

AES-GCM NIST Validation (AES-128,128,1024,1024,64) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"90a59f6b0abf932311f0b65623c17740":"be5a948a771a8
df12adaf74d702f064a75f6483c03203365fbde7d184844fe6dee0b84cf344be05b1d163817ba1516fcb87b9167ed81f88
4ada73b0058e2b38cba515bbbe462f4c21f8de1d41bca2cf4340aa659f9f07886c2bb620d9c3295318c07fa3c17fe82424
09359c08bcb337e5cf268880839b6a20f4ee4b3f04e7024":"20778bea82a6717038e7064f48a31981":"4022d04f1454a
72d2efe57533bd32757595220b20f3a37d166cec0412fb1eb2588f939ecd906c805f4827338669888e9f730905001eb1
b136b95e306edf70d9ba1e5cd0aa13a25a1f28ab55cff36f9cd7036c735e3b285d26002ad2ed1074b566e252ea3ec8a9c
e10882375dc3f1d9676e301dcb179eaae991120b796cc35648":64:"dc77c1d7e0902d48":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,32) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"6be4ef629f0b38194c74f7b66418922d":"b67ea20a320f4e
c0e4185c62a4ad79a3c97a8189a5e4d1deff9d3edff0f9a9323532853c1a2a2c1e62e4d1afebfcdf1d8461921ea6017503
80e63b912d8b7389198f976851d88a19f1aa32c97143668ad00838d98da1c4f2be0e6e2dc964d170d7f7ad2e2997982e
5ca110e744b6e10c24ca18eadff6b129b1f290c8a7e0a593":"fb77a4b9b246271abfc656433f87628c":"e5d5227725a19
a3050fbf2a97a6e854bc1218b94a4a3403b721ace3447daff68fff5553a26edd41219e68fb61fb9e964d0a3c29796251ae
4eb942187cdc55d13a09dfb487e93d9e2072d7271456a77c6ccb81154443eea176314d6e3a08619b52cd880f1c28ae52
14ac0090a3855dbd74f87389fe8afebd464330fb683dff81a":32:"3d8fc6fb":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,32) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"c50e37244931e8debc12b3d561c83ba2":"b9abf0796f2d2
f774735546cf809030f65ed0c7f6bd469ef2fe0ef32aa0225b57fbce07c36017bbc1806a81ff1a429278160a07643f8644
85b4e0e35d57553dc1a131e32aa10f1f91d663b10f0a418f472ed7b4bca54fd7ffdbb22c4d7764d94a7ffd047306144594
31eb64335b9b65363de292c04275d40a7b968c0f5c486e9":"6c0b1fd7ab424a6883c36457d1b5521f":"516dc25f6452a
e169ce293c5cee440de47353ca5ba770dca0f04175950e87a2d4c3f84fbc6eeacaac43685349292968006 6f959e74de4b
736ab924d8367b90aaa6e9492561ad4b5aa78b6737d562e960edc3b983e2e01a186e9f22896f48d8dfcfb6a42cfe2c600
6c687a27772820a1e8875bdf09e8104248ce4db883376bc04":32:"7d4393f0":"962509e494f10269b70ebad02b0cd799
d1d41191a734863ef502aff3d3ba48dc2acf9da9a3fc3f40be4d210dc5e128bc00499aec57aa0a4669863165428687b88
d46fad41e36af8ea6605586eaa5c0736d0d53b9d523e0cb5a0b285048e060a73cbf4b587d2cd787debdb2b4c8cda731a
61a15b19fe8b561fbdd3a7373853ae1":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,32) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"8531ddb03977383405baf2ee9ca7d64b":"d90c9e26509bd
ba9b1dea8d2b94f2b1881d22c2bd756ad23cd61944710a1c1f2807170ed47a6870ae654e44757fcb3822ef28b37946caf
c07284f8a0c22ae3552954f0d87b8d8c825bd546935b494cacb4262d9e2a88f254f200ad31367d8b3715afbabea5f3421
4ffedb14d7c84806022aba2dc8f88a314ffbb24017d1a9b9f":"baf623867d6a25fd85d1f08e599c0566":"18f92cdd37dcd
7f99b06838f3f68748aba367baabaebd0da9ee787d70e752fa07dea553a43b643b8d8f460175c0746675205e20a7a98ac
fcac864d7c4cf5ab4c41c031738c76882acda003c5af47b1c4df8894a827a317935d970d4afaee17715c9cfd1883e8c345
f19d1f89e229b8edba6b4f53b86d8da1c0f159afb83b6b33":32:"2fc9de46":"FAIL":0

AES-GCM NIST Validation (AES-128,128,0,0,128) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"862dd5b362cfa556ca37e73cff7f4a0e":"":"81530a243655
a60d22d9ab40d2520447":"":128:"3b9b2af54e610ed0b3dda96961dd8783":"":0

AES-GCM
NIST Validation (AES-128,128,0,0,128) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"3452b7bc100c334292e08343f139b9d0":"":"8f92739a30f
e4ba24079f5d42753d6ac":"":128:"0eeca69f8b95e1a902cc3ab1aaa8e2af":"":0

AES-GCM NIST Validation (AES-128,128,0,0,128) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"31a0cbaf21b943f8badc939e94eac7eb":"":"d5bb2c4eaec4
7088230972ae34fcda9c":"":128:"580e728512c8e44fbb3fe2c498e05323":"":0

AES-GCM NIST Validation (AES-128,128,0,0,120) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"9e8fca537746e7cbff97f1dcd40a3392":"":"43e9f2bf186b
2af8cc022e7c7412d641":"":120:"4465a3f9d9751789bcef5c7c58cbc5":"":0

AES-GCM NIST Validation (AES-128,128,0,0,120) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"35b5854ca83792ad691dbda1a66790fb":"":"cff61cf9b32e
a30cf7e3692aa6e74bed":"":120:"726793199df533dd9055b0ac7c939d":"":0

AES-GCM
NIST Validation (AES-128,128,0,0,120) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"07259267c1c6a015437a5d8cfa92f9e6":"":"18b9cf2ad7ac
e6ec1c8366b72878cf20":"":120:"4340f6263f0ba2d82c2eb79cb0cc7e":"":0

AES-GCM NIST Validation (AES-128,128,0,0,112) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"fa1df8955aa3ef191900b06e7c1b7d46":"":"6928c138c98
a4350c318fbdccd3f44ba":"":112:"7c89d9e77515d271b6ed54c9c4e3":"FAIL":0

AES-GCM NIST Validation (AES-128,128,0,0,112) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"c04200ce41ce77d772babb206315ec7d":"":"a885d58f0f3
8f9ff26d906fa1bfb12f4":"":112:"9ee0d025421f2bf18caf563953fb":"":0

AES-GCM NIST Validation (AES-128,128,0,0,112) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"650df049461be341c3099bd1613dcead":"":"8a4ff6327b4
9d297248ce2d5bd38afa8":"":112:"13f067ef0d7b448d56e70d282fed":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,0,0,104) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"ee61b5bf5060fcc637dc833926898508":"":"b2dcf21f9ffa
4a883044d29f087f9b85":"":104:"9ab1d66666d4dea3cbb5982238":"":0

AES-GCM NIST Validation (AES-128,128,0,0,104) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"01cc56ca7e64db7fbef66236a5c49493":"":"8ea5b630041
89792cc040ef18b37e550":"":104:"d685aeb54aa129a21bed17766e":"FAIL":0

AES-GCM NIST Validation (AES-128,128,0,0,104) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"134dd72ac8e28ab46720c2f42284a303":"":"c6368e4c0ba
0ec90fa7488af9997a4c7":"":104:"4ad9cdf19ff7d7fd7e273efced":"":0

AES-GCM NIST Validation (AES-128,128,0,0,96) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"180c04b2bde6901edcda66085f73ecd9":"":"9193b206bea
de4cb036f01a9db187cb8":"":96:"530f5e9ed0879ccef3a7b360":"":0

AES-GCM NIST Validation
(AES-128,128,0,0,96) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"aaac85742a55ffa07e98106d6d6b1004":"":"630cd8ab849
253c4da95ac80324ecc28":"":96:"37911820c810e3700c3a9321":"FAIL":0

AES-GCM NIST Validation (AES-128,128,0,0,96) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"ab663c4f8f2fdc7d5eabf6ef26169b4e":"":"86e610066992
9e329a1d258cd3552dc9":"":96:"958d6141f7fb2b2dc7d851a6":"FAIL":0

AES-GCM NIST Validation (AES-128,128,0,0,64) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"0dd756d49fd25380c4026ea03cafc2da":"":"6a6f7e39b0d
730ea1670e13d16c12c28":"":64:"872ef05a28da5ea1":"":0

AES-GCM NIST Validation (AES-128,128,0,0,64) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"bd8a834b288bdc7578b6c6ab36f5d068":"":"aa77de0af5f
a4dd1ed2ada5cb94813a0":"":64:"c5c094e83755f2b6":"":0

AES-GCM NIST Validation (AES-128,128,0,0,64) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"020d280dbd06939bbb5e6edc6f6d39c6":"":"09aea6f0e57
598452719d6f63b6fe5a0":"":64:"05d6c56ba601e85b":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,0,0,32) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"e47f41a27a2722df293c1431badc0f90":"":"227c036fca03
171a890806b9fa0c250d":"":32:"86c22189":"FAIL":0

AES-GCM NIST Validation (AES-128,128,0,0,32) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"9d3e112114b94e26e93d3855d4be26bd":"":"99b9852516
0c4bb2029da5553ff82b59":"":32:"33bee715":"FAIL":0

AES-GCM NIST Validation (AES-128,128,0,0,32) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"5b4b7688588125349fbb66004a30d5d4":"":"b4ae363edb
529d8b927c051cf21a2d9d":"":32:"6a920617":"":0

AES-GCM NIST Validation (AES-128,128,0,1024,128) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"c4b6c5b8e21c32f36b0ae4ef3b75d5cd":"":"3d1036bf000
0e6f1b77a799f2ef32dec":"1cf2b6cbe86a87b4b5bb3cc50024aeb27c48143658d47b41f2f20b87ed67bd6fc3b85a3a80
3f66d3576608f5d6ce6cad11e02fe12de5390722dccb8242e1dd140051bef51aa9716c860d45d45bca6effbb1a4797e6e
7406a04db5d823766c0f011ebc28e9a8cd4446ec8a75ea8bdc1b2fdbb5cc364fa9877886e30404593df34":128:"a49725
014c214ef7cc2d28b9b2b53da7":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,0,1024,128) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"63c3f81500746eaf383fe3975d84f849":"":"0799d4152fd
73c1604b4610cf7171fe1":"cb8248e5f904cc9ccccf6f273fe621eee1b4d7ed98480f9e806a48b84e2d6a733772ecf8fb7f
e91805715cddab2b462b89f6e6c7cf873f65031f13c357d5f57b00b7c391c39e78ad1ed94be236ca0ae316bce11bc33c5
d701fdfc58abbe918b9c42f7b3d6e89d46f9784b388a6e6daf47730b9fa665d755a17e89932fa669c44":128:"c53d01e5
3ee4a6ea106ea4a66538265e":"":0

AES-GCM NIST Validation (AES-128,128,0,1024,128) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"b0c88b191ce6e8e4a3941f7960b7eae5":"":"e2a899961c3
32c815685c553351fa519":"308bf10570af48d632911f3641dea60d78046211c01a63bb8e4e5cbddfff8841d2f2b11e18
ccb2170805ef4cacf7804d64e0feef40731a1704907f33b77788c18ccf35b224ec3046a67664ac9a3481d2385b6ddeec6d

a4f32423f94ea9663a5c51cc388cef33744a8159b4fb654dfdb5092718bf926c824be31197f07f276b5f":128:"92604d37407aff33f8b677326cbb94fc":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,0,1024,120) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"c818dfa0885a09f65ef78712f5ce6609":"":"ca279284723530fdd68ae880e0ce775c":"2a562abdbb483ca5f355f9cc1c5e607bdd624a078a76b717ce0f8f35d0d4c54b629f372f15d20c848d01420c6af5a7040d42063704a17b46259dcc53723caf2d4bf556143ff9117c752fa4f22c9c155c99b7bf5949d089cdafd562165b9cbf53ff51cec21f49128c8a599718bbcdb4a5d705d20509c44c8945e2a133164b9942":120:"20e9a3a98d71d460743e1efaab13c6":"":0

AES-GCM NIST Validation (AES-128,128,0,1024,120) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"2354c6b6afaa883e7ce91faca4981f8b":"":"604f2730c756c8c39a0527093bc2feb5":"959b4b0b9ce2e9120b327d2d090117553999ee10bdd384a546fc6de0957ef4b447daf07b3d07ef7dbc811f36b0fc09a175d26e4d1263cb5e21eda5ecab85d763807bb20b3cb6ac3f31d548dff00aae058d434ebcf6f7e3a37f11324134f453dd0ea7f51094863486426ff1706129a5a93c53d8c5ccb56cafa5881981fe233cb0":120:"3588c9aa769897dfa328549fbbd10a":"":0

AES-GCM
NIST Validation (AES-128,128,0,1024,120) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"b0af48e6aebbb6ff5b7c92bd140b085f":"":"d210d6502a5221ac1274a9c7f5a81725":"d725311ca10eb4b4aa24e6dd19c5e72dc34fc1ff53feb25d924a9b7d8d72205790ca4b1275bd93ad60c27a5587a45659bca07c111e9748fb683a03465153ffd735b7d134b479674ab8596f0596496fe2090f623fd1e4dd730c5283d8b172db8a25df42d9b34f388ed32676a56b8ba03347e47379702654508ccd0a21ff03516e":120:"e6222f068a1e18f09ba6c771eabd86":"FAIL":0

AES-GCM NIST Validation (AES-128,128,0,1024,112) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"a05fe482fe164b2eca7f6c3e377b39d8":"":"145327bcc10335fccb93afbf4b17e6e7":"ea6f2e93b5e1bf127d40440b8d6397405246b1b48eebe16964f18928f6b4b8ee2c36322d7126905c1a5b816996e340404b586edc2d77afac11a6c1266511f9eff1a320b035442d4078f8e42ca63cf26d12a971a7adf4645d1bd9a8e4d0a20722f7c2d529beaecc4033f7738075e1cdc6d8a929da5582540678935b82e7b7ba68":112:"3900bde9fa9ae2cbeee54d04f224":"":0

AES-GCM
NIST Validation (AES-128,128,0,1024,112) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"dacbadf819eb16a63f6f091d13ed04d4":"":"b9ebce724b0dcb0989ac2d8e7ff8aaec":"7dc6e2189d8a96f3507e352e05e8fd1b4bab988c2f1c706115887119f63b78084f015d85f6b460901a02880103e4d36e8f6527dfd74e4a3acd3f578c0cc726b528875f701ff8b66e5c11b4689c346a098e123bebfa253362cb86829be73c2b85a6881fa976aa730fabb76775027feec7fd920a6c8965a4a509ea812d7c413a95":112:"8988fca83c8cfb1f8feefac46f04":"FAIL":0

AES-GCM NIST Validation (AES-128,128,0,1024,112) #2
depends_on:MBEDTLS_AES_C

gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"969244c7444f3f3bf193b28f8e8e96dc":"":"49b2845a1a1c87fa66eb8f78c05ac029":"1414a07e86d8b61d1eff43e1ff4ab42c1c95e159058b74c731e3007d21a5eb78bc17b7e920363a3974aeb8608813dc9a4655199b6703ed337450702d8ab16a89776831b2c7c811fec3acc23598a0aa01680a7bf42a4e258145beb08c9f0eacf2bb5f56d26bea3ad11e1a956a630b80f3d22bf35592b4704f7c464b08b06dd7f8":112:"a291c7527385f037f62e60fd8a96":"":0

AES-GCM
NIST Validation (AES-128,128,0,1024,104) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"525abe490c8434802b69439c590a5290":"":"141f79f0501316e66451c41c7af0f0cd":"be440db66d3f81be467605a7b2805ec1df5e71e1b1b04bd7a4d05e912f5aa1912ba08de72df18613b32b7edf78963c48c80c25178b3b19262b85bb829f5377e0b368b500d6d3b442f54172d4ca4500eb5b4d478b602e5dc11d090539455087ce1e5b9ea74355fc06e9b60cbf25a9804d3f8c623fff130abc48bc2d8d116b8366":104:"038c7e95f790e6ca5ce73f9551":"":0

AES-GCM NIST Validation (AES-128,128,0,1024,104) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"51644e025659de983f5c8156516b812e":"":"614837c743d0974e9cca497f13038c02":"60c5d062ade2c5c2dec68b734dd3e58ec474a586d1c4797fdfa2337800510134cb27a10d501927632af3c1febc275010c0d2e5abee630cd2bc792963fa82a42286ab047b934a261927311b40f5f953bfd661427921147cac7613d95ee86e16326ef67c1ed097e8fb87a78753d785de34e03a182232786079cb6be00182e41c9e":104:"77e3deba2c7f9386f85bc4a801":"":0

AES-GCM
NIST Validation (AES-128,128,0,1024,104) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"08566ca7310302dfb84d76ea0525ba20":"":"5f20ec9c35c08aa7f1c0e8a20fdbd2b3":"5d84e32768b8d1e7e3c426b3118d48e35491bf1bb454b359c8429220216efd8826be94fe1919409a128ccd8125a594f1691c9421fc3dbbb3f757bf2355bb0d074ceec165eb70e26eb53fa2cb5d84dfae06babb557805ef7b8c61c1bc76137571bcc5e84bf5987dc49013831d78bd497ccc49cde7dca2cb75e7ab967da8c6ce81":104:"873f037fc05252a44dc76f8155":"":0

AES-GCM NIST Validation (AES-128,128,0,1024,96) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"dfb54db96383fa911bf5b4fa1218ef9a":"":"7e849e24983f63f1194b396bbd2d55e0":"d3fb689c5818810dd104693f3306a10b27178444af26798a194f7c2ab31ff3a172904b951942b1a26c8ae5b5b1ee2d86dc78bb72a335fde350766d7d9aef6f549871dd46b04b2cc319fcdd47be437d431ad18cab82d51ca9fa57f4108a8de622a92f87d28c0349fab27757fd773413f559a8c00d30e258c1f6cd96f9759bd957":96:"dada7fc7fed58db462854ef6":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,0,1024,96) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"389cf888474e9403e5f4d0e22ffec439":"":"ef57794cf6fac9f9cea3e8499b53b1d6":"7ea7f7f4763ad208eb6199285b6b2819756c4e3caf2d0ac6f5076ae6785fecdcc4b138a51860ff8b87aaac3a18c2df778a4818308d458dba28f5017513e1454f60be20dae68736ea6d48b1f9deadb517df63140acbd329fbfbc9b82f3ca1862c9e998f0faff1d3ae60b005bf66829f5cf0c5fa03efbdd92d39351e3954be0257":96:"92726d90ad26130e65f2beb4":"FAIL":0

AES-GCM NIST Validation (AES-128,128,0,1024,96) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"e55abb2ca36c822bf2a030ac703cb8b4":"":"d86f7177e8e
c90f9e9edf10175d5012d":"777a9d93091de56324c10712243f5541722e0b27e1f303fef6faa387a8666161ab354dbea6
c43c82a24e8623bfec39aab13164add6be0dfd55d23204c0975b4ba6fbda51363befde482a9ccc1eb9f151e6ad59c77a1e
24dd268389e4686f198a936dd603044a3fb653d63cff80597f5a2913c8a2ec1b7d9dce5728dd56c78c2c":96:"65025250
343ed8c09b3fceed":"":0

AES-GCM
NIST Validation (AES-128,128,0,1024,64) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"586114f3b1dc087e1b2739b28c592dfe":"":"ae5a38ddd45
5505284434a4bcfe81ef2":"531ff8c285e532d961f49bd210a5523cd9b19a697a3a3fb26db940a496f253862405b1e825
daeda7eb0445c98022b8342c8f8ea20301618483f8ab04b6ebccd7e7fc57878fb544a5bf78fa896f50ac30126ff8afca8a8
6388666b64c643d16812729bfd7e5c03ba52f7e6ea4c6a685404f7bcbd956964417fa0ea9a6d7290c41":64:"467a8156
10faeb82":"":0

AES-GCM NIST Validation (AES-128,128,0,1024,64) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"cbfe806bddb7f06b3826b097550c68f5":"":"04c1b6c9fd2
ab76fc2adfe15d3421bbb":"cfa86d02599652cb4ffff027b9c6ef2336dc9fe946f64fa5ce83f624e144563d4738381bc537
1c3cb55cf41ceda07e62cb635ff37246bfa428785229c6e869d5df69d7949a8577889a29e3d05b788ddd43608d9c14e3f
1b51ce2085b9a976fe843e3396a74922babe6797d5f01c37ead623b5b582505bcd29edf8a6ea36b0fc7":64:"0697ac372
a9acafd":"":0

AES-GCM
NIST Validation (AES-128,128,0,1024,64) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"96ce3a095a91effdd91d616f1f02ddcd":"":"579d6633ec66
87afa24ef874899b58e0":"3ff3c0038148ed391b6a10aad623a82fe9209c5ba74482f11506d597b5fc7af977235d8ee9e2
8cf2160346ddd0e33a5bd1fb67b87dad7167fdd4b2b4000d8460ef7b3e1b59b9d61d06cfbe7945379ed6b650de86f396
a38cc70d47b8a349f067d00144c903c276b323be6a929a7d7dd8ae7d254d640cdc1176f98e01a1d8c82f":64:"55a0f610
32e048f3":"FAIL":0

AES-GCM NIST Validation (AES-128,128,0,1024,32) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"24ece168c2971cf2b404ea206dc9e29d":"":"e9db62a4249
1664a6c46cbb0b2bafc92":"3579f6c0cb3d2a5d0c4548855c7c052d36b6a8dfc60f4ca1b4bbe28ed87306119e71982dd
84c4205ceba918d675472753df1b5192d3693dbf6a061c6056e312135ffc5ff426895a7e30f7f675d2cb21de06eea5e376
1b94deef7537b985d324864c9ff6ab6e230a1006720f98c958912b604a6d03e3979887c07be3ceaafc78f":32:"d2b15a2
3":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,0,1024,32) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"d3c3cf993f6740a019e61ce13c29955c":"":"af900ac34808
2ff32d2e0ab886079516":"2ddd0e8c99661f0757f04aa79a1ffa24ad48fbe5da68b9e71f7a0cf1b4f2ca9b757695900b75

49d48847ae49950dc9b270b1569d29dcbef412216737bd83509c17ae41c34ccda318939cb37a0a380762993a7568c0b
07794e78746173dd5c0d921cd50de4b548c1589e142c3dadbad42161aaeda2310f3c6d5c722d9ac69e96d":32:"f2d3a6
ff":"FAIL":0

AES-GCM NIST Validation (AES-128,128,0,1024,32) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"5f1e5bd45ee8bb207ebbd730510ff218":"":"8846424a194
f5de858556e6be5b65d7f":"e968947fc0e49136e730b97f6b16e393d5e4fdf3e4803a23af79211ef59f29167c60ead72fd
489da32d2ffa43b2bca2074f9d1b4f5396ca65004b0806cb7c6dfa751fb6afbee3e443f3c9b0e3df6722e0d1320441400c
5ca508afb657c2b7f1669b0de21761dccab9a40fc513768bd1f552692626ce35078a2e0e12f5d930647":32:"0d6c15da":
"":0

AES-GCM
NIST Validation (AES-128,128,1024,0,128) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"3997050377cfbb802cc438d973661688":"b02f0dd373e42
c65e8e1db2dd76a432e0b2bf6e630c8aaf0d48af51b3709b175de9a19b3245ae75818274c771c06fae225c4f8b0022367
12336e805ab006449eb29cc5e29abd82b06c32d4c36ee99acb9a6d7d9eae6ec6ec263c002a22c4a898c74f6abd6d9211
2367ca7ffe82787c5b39e7012ba22825d3612af3d41e8008a8":"c95c84c263bdfd5f1de66e7e616cf3fb":"":128:"b35b3
cf6ed59ccb69dbc9b47a3f284ae":"FAIL":0

AES-GCM NIST Validation (AES-128,128,1024,0,128) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"c58583f6479d9bc9f1bffddefee66e59":"564a9f700cbc1f8
95e4f4fa6426f73b4956896a15e6127e7560d74e3fd0b980d2ee45b7a6a3884fa613d91d13921e3f90967d7132bdafcd1
46dd8ff7147ed1964c2bdb3e12f4133d3dbbc3bf030ff37b1d2147c493ce885068d9ba5bebae24903aaac004aa0ab73fe7
89e4150e75ddc2bde2700db02e6398d53e88ac652964ac":"cee448b48d3506ff3ecc227a87987846":"":128:"361fc289
6d7ee986ecef7cbe665bc60c":"9cce7db3fc087d8cb384f6b1a81f03b3fafa2e3281e9f0fcf08a8283929f32439bb0d3025
16f0ab65b79181fc223a42345bad6e46ff8bcb55add90207f74481227f71a6230a3e13739ef2d015f5003638234b01e58
537b7cfab5a8edac19721f41d46948987d1bb1b1d9485a672647bb3b5cb246a1d753a0d107bff036ac7d95":0

AES-GCM
NIST Validation (AES-128,128,1024,0,128) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"0bc2bde877e881aea512068105694968":"1a6369a45e8ef
2846c42d54f92d0d140a94f9633432782dcbf094f1444a1d006acd07ef6076cd0faee226f9ff14adc1fb23e3c63ed818c9
a743efbe16624981663e5a64f03f411dcd326e0c259bcadca3b3dd7660ed985c1b77f13a3b232a5934f8b54e46f8368c6
e6eb75f933196fa973e7413e4b1442b9dee5e265b44255ed":"05f0c34ab2e8e8026b0a23719344b71f":"":128:"46bab9
fc2dbe87b8f6ca0ed4d73e5368":"FAIL":0

AES-GCM NIST Validation (AES-128,128,1024,0,120) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"e14f45ba5d1eb52e0412240da5d7b5f9":"9a85fda19ce923
f093a0c25b0c52f5d9534828af7c7687d22307004ae2d10c4592242c0f2704070307ab55b137780d1e2013a19396ab43
ff6a295b63fdcf323456d149758f9a2bb37f1418d62ea6368b24d5067b9c63d2968e06d6586c7e3275faffa005f7c7bfef5
1303e4c2b2ed4564acd17d50efac9f5e3e7f16ce589c39b":"d7f8ef12f66f8b7c60aea02ef6ff688f":"":120:"beede05e49
28c808bc660f3de95634":"4ad5b9ace0c0c7c07df2900faf37a902899471e7aa4a0a1ad5387f8f56d73f78f619be79a4e2
53f95b15d52895a05bae9ecffa916d35efacd8baf1c704d2aa4a38c234efc4dcfb191ec0fa0b522328fa5b5dff55e8c443fe

e660ebe3d8ad85de157a889aefc823720030a4cd6ba94a6309dd61806f0abb27772432018bc61701":0

AES-GCM
NIST Validation (AES-128,128,1024,0,120) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"9a64579f3601b0022d357b601cd876ab":"88be1f4bc8c81b8a9d7abc073cb2751e209ab6b912c15dc094002f95a57a660b9f08b1b34f5947223205b579e704d70a9ecb54520ce3491e52965be643f729516f5cb018beeedc68a7d66c0d40a3f392ec7729c566ce1e9f964c4c0bd61b291ccb96e3d1fac18a401a302f3775697c71edb8ff5a8275a815eba9dd3b912e3759":"515efc6d036f95db7df56b1bbec0aff2":"":120:"13ea92ba35fced366d1e47c97ca5c9":"7fc8565760c168d640f24896c69758355b17310dbc359f38b73fc7b57fe3f4b6ecad3f298be931c96a639df3c5744f7e932b32d222f5534efb8eb5d5b98d218dce3efef5c8c7ce65738bf63412d0a8ed209071218a6fa2f7be79b38d0b2f5b571ec73f1a91721bd409b1722b313683e97d53df19ded95fd471124fa5f294a4bb":0

AES-GCM
NIST Validation (AES-128,128,1024,0,120) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"1bda4acfd10ab635f357935bb0ab7020":"c9ac8d4ef7d83848fdc03664957c28b9b76710797d5db1c21e713e85eb0898892223e52be1644fc7362c95026ebb9c9ca74d7d3739eff10cab1eda00c36628dae0b98d119a14635800e37cd340faa6fbba9c3d41d52722cc3969612b1a8c5ca9a68773f5ee654506cb88ea65fb1eddf5ab6312d0170dc03324e483342448b854":"48b77c587616ffaa449533a91230b449":"":120:"8325e4394c91719691145e68e56439":"1287ad3719508a9be70c19e3b134a2eaa4415d736c55922e9abcfd7f621ea07ffb9b78d8a9668c74bbd548b5e6519ea12609d2d6197c8bd3da9c13c46628f218e7ff81884ff7eb34664ab00f86e09cd623bec248d8898ef054fce8f718a0e0978e8b5d037709c524114ec37809ac3fd1604e223e08f594e7aa12097f7dc1850b":0

AES-GCM
NIST Validation (AES-128,128,1024,0,112) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"d21cf24bc5bd176b4b0fd4c8477bb70d":"2e7108fd25c88b799263791940594ec80b26ccd53455c837b2e6cf4e27fcf9707af3f0fe311355e1b03ac3b5ee0af09fb6fb9f0311f8545d40a658119e6a87ba8ba72cc5fdb1386bc455c8fec51a7c0fec957bed4d6441180741197962d51b17c393b57553e53602f2a343a0871ea2dc4b1506663b2768ce271b89c4ed99eec6":"208cb9dced20b18edddb91596e902124":"":112:"7edfb9daf8ca2babcc02537463e9":"FAIL":0

AES-GCM NIST Validation (AES-128,128,1024,0,112) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"3d02e2b02170986944487cba8448f998":"bc1d7553f4a28754cf59ed6f7a901901f04ce62a449db2b45ad60329d0341bb9ba421c783c28a9200b41da8ab6328d826293134a7d0c9a5775dd2735e7767efda4ad183566e0847d6d978abd1a8ab13b16b8323acef05ced3b571631e1e24ad44d65e6ffa64e03c9970e94bacb9f721aba06cda6a08806a3be63dddd8029301d":"6336077bb83eff1c9ea715de99b372cd":"":112:"0466bb2957281f64b59eafed3509":"5f395958f2f7acafb1bca6d3a6ec48b717f2ceeac1b77e1b0edc09a09e4a299d2ec722cc7daf34c8f4121a93c80b2adb20a2fc95afd09320f91085c93c8b082dd703814c9777501d23bf9b328f07f04652592dc5a3f4321626a695b8db8e65c8617c809eb2978d8c9a882ffa82a4bb707c1a8f9a965bdacce5c041bafc94a1c6":0

AES-GCM
NIST Validation (AES-128,128,1024,0,112) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"cd1ad1de0521d41645d13c97a18f4a20":"588c2617517329f3e1e7ba6206a183dc9232e6a4fa8c8b89532d46235af1e542acaa7eae4d034f139b00449076ba2ef9a692cae4229988

78dabdac60993dce9880d280bec1419803ba937366e5285c4a7f31a5f232f8d3ef73efe7267b3ef82a02f97d320ebc9db6
219fbdf1c7f611e8e5164e9ecf25b32f9c07dfa12aa705af":"413873a0b063ad039da5513896233286":"":112:"d4dbe9c
ae116553b0cbe1984d176":"bd519b7e6921e6026784cd7b836c89bc1fa98e4013b41d2bf091ef0d602e44a70df89816c
068d37f0c6377af46c8bfa73ec0d5bc0b61966f23e55a15a83cea49f37cc02213b4996f9353ee2b73a798b626e524b9c1
5937ecf98a4eded83fb62e6deea1de31e0a7f1d210f6d964bc3e69b269da834720fd33487874489b8932a8":0

AES-GCM
NIST Validation (AES-128,128,1024,0,104) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"1cb120e9cd718b5119b4a58af0644eff":"4c8e8fb8c87ff6b
994ae71bfbf0fa4529f03bad86edf9d27cf899ea93a32972640697e00546136c1dbc7e63662200951b6479c58ae26b1bd
8c3b4f507c0d945d615183196868ec4f4865d1d00bb919a00184e9663f6cb9a7a0ddfc73ee2901f7a56ef2074d554f48c
ef254be558fca35651be405f91c39e0367762b4715d05fa":"5a7087989bfe2f6eddcb56fde4d72529":"":104:"95d8bd12
af8a5ab677309df0fb":"FAIL":0

AES-GCM NIST Validation (AES-128,128,1024,0,104) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"315b206778c28ed0bfdd6e66088a5c39":"6186f57a85b65
f54efbf9974a193012b1396fc0ca887227e1865f1c915ac2af9bbd55969f7de57ce9fb87604cf11c7bc822b542f745be8a
101877a810ed72bf4544d0acb91f0f9d3c30b6a18c48b82557433d0db930e03bcecc6fb53530bfd99ee89f9e154aa1a3e
2a2c2a7a9e08c9aed1deab7fae8ea5a31158b50bca2f5e79":"7ec6f47ec56dda5b52bbdaa6ad2eb6da":"":104:"930750c
53effc7b84aa10b2276":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,1024,0,104) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"e886de1c907c97e7db8ec80a79df90f8":"c64cc9596d7c73
8746ab800f688eec190a4c802c55b2528931d74d294496892b81f53d3073d48f9bef1d58ce3be26547474cdda2868abe
ab71aff566fff613b4e5bfed1be1d2fff35d8ffa33302d3da1c82e421aa3a23848f31e26d90c0cb2ac2ae136ada73404ed3e
0e1d3e7cb355a11cd2a4f9393b4d5eac988104fe1cf959":"612cacbf33266353d0a29a24532f3c0c":"":104:"76634e58d
8f3a48f15875ac1d6":"7001d7395efb432e2804cc65c0ba5d4719ce84177ce46292c4fd62a5596bd2bab1d5c44217ac4
3235bd94489c43d01618a11f047d2e247062c3b88d6e59adaa1f46514fb33b7843483920bee60a41f3cb312322c305d2
5251b4704fb66da58637c95a9d539731434f60ef44fe3cd6d37e2c8e7089880a563938dcc98b43f08fd":0

AES-GCM NIST Validation (AES-128,128,1024,0,96) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"3b936e09a6477f3bd52030a29df5001d":"65cf11d1afad19
b34f282f98f140315992392f5d4eed4265085b29e1e5553f4783fec681ba2d368486ba6a54c00e71c82c08ca3d097904f
021ce4b0acba2d2a7005e28e5f8750ea3d18a4f78363c37583e85104234498942c639a0564b0d80055c21cb7735dd443
48298291ab602f345b1d74d624750c0177fbd5cca6f99223b":"f93105be83fa5e315d73acfdcf578de7":"":96:"91b55bb
5e3f3f1abcf335db5":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,1024,0,96) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"dc9e2095de7b1b48481b56bf6a3604cd":"ed61ff94a3f84c
72147faefa615e2df00324fb01790cf9764c72c1b8ba47f17866a1fd64ee5c2f53865d1bc24ec93165a6774466a5960319
9ee476c1f2da7d932c8943d126aa172d532d8475a484d42bb45fcf92766feafd7f3e2e3d42d22f6f84a90e7e688232f799

d80cd2cc152ddd21ecfb137701ecafcb2b65abe2e4e6f4":"9e5268db19a1b51c0496a160ca76f8f7":"":96:"0fa9588536fca71bb44260f7":"ef562e301fcf923ff1a1acd3aff9b1c963058228655fe8a66cab01396547dbd2aa1f79a22eefc62944b86d1a31ebe2d17130175b8c003d6755b0eb8b79895b0f7f8046c5ae888a067ba17bc8e11a8f6e5023a9cd42f6461966c28e505b371c0f72a2606bff430a58016e99713d25ce11f10391fb4a922e27989422c6a64f9107":0

AES-GCM
NIST Validation (AES-128,128,1024,0,96) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"3f93901fd7cc88db3ba76a158d658c7b":"16402fded879fcbfe9405902aa63ca2a520889e0045f687455469b7bb867829a01208b8dc5dcc852d8ee478993c30e6d9ec6408773b367821310a0ae171d38d71e06981ff6e845acffbc794142b87c748e12484c0636419d79be3d798cde59e9dae0a4a4a4346596427e6b235ad52e6a1b02d6f4df0c7de35fc390cae36aef14":"7e98de461e6d96c0ce6c8d8b3854cf49":"":96:"86c9a70e4bab304ae46e6542":"1b4c09569b42c469b3ab6b39312c214502ec09f5fe2fed1d1933d13cdc6a7b77a5d135123fa69d9207d6844b0357b26b7a2f53b33a5cd218dacda87b78b09cf259e48e74076812c432e2d0833fb269721f9347c96e158500f9b2283342a35c8de0a022edce711118d72d8fbaa354bfb0ffee465844ef2d37e24ec2cea8556648":0

AES-GCM NIST Validation (AES-128,128,1024,0,64) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"42289f3d3cd5838e250ef54b128e60d1":"3edae1d554b67d2036f5fdbdb2945cc112f100adc1b47009c2e23f6a2eaee78d1f39ce8a98f715853cc29fc793fb6981ec3036834188dea7d668185ccc8642071b15de1332f6a59c8a9b4399733eb4b3d8f224af57ba6b4a8e64494bb6630b9d28e7ec3349064350febcef6a3ad1d6cca1b1da74f3d2921c2b28a2dd399c3416":"e557389a216ad724aafdab0180e1892e":"":64:"6f78bc809f31393e":"25c476659cc7b343a69088baf868a811ba37daca85c4093105bf98235a90aeca015ab034da008af0982f9b2e80df804c186a9b2e97f74cffd70ebb7771d874fcaf12f6d01c44a8b0ec2898cf4493cf09a16a88a65cd77909bbf0430c9603869bd5f20d56cb51d8a3f0a032fc30d925c96599d296b1ec41c2912bda426adea4fb":0

AES-GCM
NIST Validation (AES-128,128,1024,0,64) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"3d772eabb7f19475665ca2a7e693bcfc":"e9fc4d86f5b857fa6057b73f967351e06f87288c40a95b9e378c84f1a4c0f4b80ed0a0b44ff90a8973be4199c0c4006fc4f5ea19d5f1fe8b9c8c01f4675ab85afab0592bb3daba36bb4fc7ed9eea867e9d8cc50c19fb62a5a57956e9efacebac5e9f849649d35a329bd68de97bb6e5ff7bef477a86765c2c9ec15e24cbba5c6e":"0747cbb486a013453fde1ca6abb11dbe":"":64:"8e761ffaea68f967":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,1024,0,64) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"fb7fd753ee6eaaf283a42a121dab4e43":"fd5cecb2c0287cb8229e97d9cc4b9885f428710528884ce663ed1728cd44cb2df93e56ef17ace0678d1e341366c652f4ba7ee45797d39be4a05c1151e5cde499e13e5d45549b5d95a174d03616d06ef96e9d7b2b6bb0d79a726b253dd64223a5f09611671b234ccf9b383952f8888814b2c167e774cfbf54e9c6b99a753f4fa9":"8164929fb54485377ecccc9b9621af5e":"":64:"40a2fa7f4370afb2":"6208d068be60f7b04b80fc611062e6caaef9a5cf59f850d174b7446c78c039ea9aefe4885e19c2b33911d32ce1fe3c48ddffa4b03e450fd35da03f40c4e7c5bb3b1c3f3049dbfad3ac81ca1b79cafbaa172f4900e3829d38edea3b64000f93924a801259bc4b2523445c64bc23bfee190b952468507fa4baf6dc2bec66fcf0d8":0

AES-GCM NIST Validation (AES-128,128,1024,0,32) #0
depends_on:MBEDTLS_AES_C

gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"30d757fd73a0fd5fa49159ad0653296d":"17d485b258f80d8924e35291118cfdcffd86c47851b65f0b06a7c1f5202de82f3f460fc61b1aa38fdba7c8ded375c92cf005afe63e59d362c0960044af39241b81ca24e85c5faa43903229355b7313fee21b992ef3931d9d2407b32b3cf72dd7acbc7948395eb513cb2fd428b215ba2bd1e29c62f45d0ce231884f62480c6d8f":"b35b8df0aebd0608517f2830e0e70cd0":"":32:"954c0e99":"022618d2598f79104e918a09c937a82b3db59243b5e13de731fcb912e4366105797ce47f6dce7f08073f2f41e5c15fd6b1ec4b5861469a4880c3b0bd769b78c696ff29c28c9349d5a46a6e5ad9211bd4b708a8c0b6928ebbb0dac1c0a5f5ce6b05de6a50073128566a23f09cc1b826aa5803f9f750aa4debf59f24ae9f98c9b5":0

AES-GCM
NIST Validation (AES-128,128,1024,0,32) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"d9d3cfd5900de5d5e2109e7721cfeef6":"e4243cc37cc32dfcedf9bb76890e706af6ab1e06b290b8ccfe2a55e5dabe68cb390f7636dc9676b431d4dc8ad3f6d989e510194294ab7ab0556789046743cf374d8b6462f5f95a17f3f44337d6c69ee47b0e1ad7e5ce6f9b224c54099a104e70d2d06af869b921ea47febe08f90c591ed49c1f12003afceabd2c7bba458a0111":"b4b9dfb013de6f7c44779e5a9daaf5e5":"":32:"2b81e8ce":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,1024,0,32) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"68dc138f19354d73eaa1cf0e79231d74":"ce345567a76bc30d8b4fd2239788221cfa75e1a310aeeeb8c355f8eea57d80967f3047fbd4e6173fac5caeb22151fa607065953c4c35e0537b9e3788cc80de9eedf2a340698bde99a6a1bdc81265319da3e52f7a53883b7f21749237fcfd3cd4f149bb2be7a4ddd9ef0544cfe0789040d1dc951b6447304942f03ab0beae8866":"e7147749560f491420a2d893c075bb76":"":32:"70a83f6f":"64b021612c78b3e192e8349d48b77d02927e7fd70c7160d37cb8ef472f6bcd9df9d93431627c1c80875e208724ae05f94fdd2e005e9707b78a1bf3bbca7beec4b03ddd4d9de6235ffd6d84a8b9a1842e104c1e22df4566f6c4d3d4e3d96a56b9b8a5cdce9da70aa236109b289266036f285564060b204dfd7ac915eea0dd0b1e":0

AES-GCM NIST Validation (AES-128,128,1024,1024,128) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"7362c86344e0aefb0cf0d04768f9c05d":"8baffc7836004deb87c0111d47c182512bf861874021ddfcd559acf2c4a51cf5bc4bfdee2d039b9c005b6af95a2607643dcf4d9cd9d62412f709334556db22fc91d7b40438505d6806ccb2f2c21ae731bc1f1c825d28a71ab27095a39985e96ccd07cfb2e75243ccafd474494a2338c324ef533ca5f17d2ac1b1883140342ced":"7e8d12c2f0dcf4f792247134234ac94b":"86d2b5debc3b10495da353d6821f6cad380776d805bd8660b08dcdb1acd87026e4f344b547a4db47b5f44cded314bec4ce9a417ce40a2acd5a21460c42dfcd27483abf3f38dd8cc5fa523b6768a26513df5896435baa97781cff1966e2e3d6ec6d0a9cdc013de5a50e4d46831667055bad04f784024a82f9cd087ae4cd37dd64":128:"9594da428fd8c1b13ecb23afa2c1af2e":"e2c424f42aedd56f0e17a39d43ad19c8e2731efc7a25f077aef51d55280b10e667e338bd981b82a975ef62bf53bc52496b6995d33c90c7ae14767c126826e3f32bd23f444ddcfd7a0dd323b0ae2c22defad04ce63892b45c176bd0b86f5fa057a3dc371359744cb80bbfb4a195755136a0ea90b4044a45bc1b069f3cb3695c04":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,128) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"58748bb204ccb7bdafdbf739b6c19a3e":"b72902c9ebb72a86be539b19a52fd9af00aa4de081d90c0d8ad580ebb5900177a036f40a1e9b43e3a07d715466526d6d7544e5a5551805b62463f956cd519fc99182c2d54bd62fc7ffc6e5ebf1503859b706da11a1b6c707a67a70789dbfc10ef726bd360f9f2347326e068e757c8443ddc9308a171e682359ae1bfe87194ab5":"93ac298c73c88e127a4d9dd81bf24e3d":"8f168fc4d1d

a13bdbefae3f9d6ac1d8cb19fcec1f43f727951af0a466d8826649a46c3cb50c045ea83849fce0eedbc042a1a435e6d9d5
9017997a2d5459b940078b8a7f3b6b0ff279ff8c560248296a17240ff1b0643d1f436b6e3f2079363fc49fb45f410debbd
de083b92057916368cb807d603cb82e2c0dc01658bff7f1ab":128:"efba4589d4a03555766bbc3b421dd60f":"d5c97a6
59f016904ff76286f810e8e92da6f8db2c63d8a42e617760780637e32105503440cdf04d1fe67813312f1479fda8d746c
8b0b080591eba83850382f600e9d8680516c6579669f0b3d0a30323510f9de1c92512790b8347751994d022156cae64
da0808a649d163a0e99e869fdf224b7c1a6a8fbc613d5917eca8ee08c":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,128) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"6cc13cbd62428bb8658dd3954fe9181f":"2c9ec982d1cfb
644ddbc53c0759b10493206d5186affc6882fbb2ba3aa430f9bae1209db2d78dcc125f3c909a54dd84fdff96c71e67821
6a58390ef4308bdd90f94f7109c4edefa76a74fda64b201b7a435bbabc27298f3eaa4c2d1393bd584f811fff52638f6ad2f
6d86a8c3c9c030d9d4264c8c079592a36178d25991cff09":"86740da7ce4efbed70af55e1d6c10fdf":"be561ac15e3cfda
624b422af97c26719c140bb50e4a993d636efe9c7f1963fb9047a0762169b571a698ff310bc417e34d4039b7562a95af7
10ccc1b197964a376c986fd2ed8ac4b0c7b4e843c37a41366f2f483c821a1823f317416c7e4f32eed9b9dc2ae1a2f3ed32
c4b3187358a2329aa42191b7c2fe87b6e27ff20303cb29":128:"76b990a1e010e5f088f6ae90bec40b32":"0b9a5f5d2e6
852b75b9cf26c1b310b2200e56dafcf3c941478862cdf9737ac8e2cb9b38d41bd4a1872ea1b4cfd51a1a0b9b743aca439
eefa10de8459a0a7a221c5429b3dee393f17031ca6c399df8e05657c3db55be9c9dd29e690042a4ed8db732efce7c58d6
b20a2a0f7c79e42e5ada43b87ab00f481c20cac1b35514dcdc9":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,120) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"286d3f5080cfe88538571188fbeb2dd5":"5513592899771
1360622eda1820c815aa22115204b1e9bb567e231ac6ea2594b4d652627b6816bdc6c40a4411fd6b12fab9a1f169d81c
476dbf77151bff13f98ca0d1dc0a68ea681652be089fadbc66c604284eebfc8ce4cf10f4ca6bda0e0f6634023db6e3f0f1d
e626c3249a28a642ecc9ec5ff401e941fa8a3c691566c0ae":"da6140bd4dc6456ddab19069e86efb35":"5d350a04562a6
05e9082ebd8faec6c27e561425849e7f0f05f5049859c2c1bd2c4682ebf9773fab6177d2601fd5a086cefc3adef5a2f8f6b
5dc9e649e98dd0a3d1a2524419f01305bd0fcfff52d84a20d1b14dea2138dcc54eea2bf263c6fe27c3e7255f1f359d0d00
fb1b350d7a04965af30027632520197e85eb41de6bb286":120:"d90d34094d740214dd3de685010ce3":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,120) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"726ae113a096769b657f973ea6d2d5dd":"90636012ba8c5
1d16f8f6df3d3bcabc3f09aeffbe2a762f62e677913188045b861b2e7d9a7bd93dcee46e9e4832e497a6f79db52b4e45c8
dab20fa568ff9c4ace55be3216f514a3284768a25d86b1c7da5377622f3e90ed4c7bd4571715af4d0a2ab5181d0475f69
9202e4406bb9cfdbd4fa7f22d0dd744d36b3223134658496":"2f9900226c97585d200dd20a279c154a":"761663c3fcbf
1db12bc25546b2425b8229b3153e75f79fa63958819caee3febff74603d99264b5a82ef5980439bef89301ae3206a1d01
a3bbd7a6c99d27d1e934cc725daeb483f826c2c9d788fd1f67a627864cf8b5f94df777bb59ef90cb6781a2000e6f0baa4f
1ea4754b47bb7cbd2699f83634e4d8ab16b325b2c49f13499":120:"d095bfb8990d4fd64752ee24f3de1e":"9f7759c6d
24fd9aa0df02a7c0cc5f17e61622c63195f85dfafa5d820d3ad218c7288ec017821100f1fade10f9bb447a4a01e3698b04
5548c7619a08f2304e2818a9bf55e70b40f8b994b7dcf0cb243848cf3f6fdfec3ebbb147d01df84a3ec62cd8fa5d78ad9f2
f28cd288a35eb49a5172339e9872e8e7e3350b0d69f59acd07":0

AES-GCM

NIST Validation (AES-128,128,1024,1024,120) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"73a9eeda721c6f292e6b399e2647f8a6":"215fc7e52abe4c751ca2f7f9a5cbde9ab8b44b8d4054bb62dcea6df5b936145ca6ec83a2b78b070638fd6e5ea3bad5d0caf1b8f755f391c3e0962a92337e3eba575585eb83680075fc818860388c587746af78d5fc75ccd0a63f1612abb1ba0f04a2228ca27fbddba4878f9b2683683f516b6d6fe4f6622e603bd3c5ad45e332":"c1e80eb723960049cc4448b66433f1cf":"fb2a0b1f817404e74aee0a6ec8f2cd86f0c9114ed367b2690c44ad80f9d3377d7fd5066beaf1daa739d27ed3fba98379188016b1fe901204a174f9ffca370c181aece5e5d40939a0d460913b40b895e78a3b80ddf3d613c05e4e27bfd161ea2ef42271a2679f2cdca5b728ffb2319781c946a4f3ecacf486b754b30bb04ea60b":120:"e08161262234d0d5be22f09e5646bf":"b5e286183f16dd9403bec6786bd4836cc6add47947ef111fb1d5503c18c333c8fe60959502f58390d0e0f69fbe5fee13c72aed65fe6e32f6ea45877fe44f8a556aa5157b112e572197c1c350b7943c6cf2e9146018599524d27599f09c86027f2c5927e4a20c63833870e8369baa36ecc07cdb3ced520b5ae46869ff357ca089":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,112) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"90dbda7397d8fc46215a1218a6ffd0d8":"4f82a1eca6c9184240f50f7e0cfec07ec772cad5276d93043c462d8364addd9a652eed385ccc6b0faa6ca679ab3a4c3d0be6a759425fd38316ee6a1b1b0c52c1bb3b57a9bd7c8a3be95c82f37800c2e3b42dde031851937398811f8f8dc2a15bfd2d6be99a572d56f536e62bc5b041d3944da666081cd755ec347f464214bf33":"7be477d14df5dc15877ae537b62e1a56":"7358ddf1310a58871a2f76705f1cf64223c015c4d1574104d2e38783bb866205042f05c86e76c47a2516ce284911f1d2cbee079982dd77167e328b8324eec47c9244cc5668cf908c679bb586d4dd32c6c99ed99a6b571cf18b00689463e7a88cea6ea32d288301a10a9139ed6092ffe298e25b8cfb6b4be8217f16076dcd0a90":112:"776d871944159c51b2f5ec1980a6":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,112) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"0c85174d428fc1c7c89ca5d1b8aaba25":"3735cbfb8000260021d1938d2a18e7737f378ecddb11a46ce387bf04e20bbfcc902457637fd152ab87017185601f32a7f906057123b6c2da31a1069c93e3cacc59a359aebd3e31b302e1a1f7d5d8f1b2917a8fe79181fa633b925ce03a1198dac48f4c959076b55bc6b3d50188af2c6aa33d83698aa8db22649f39825ba54775":"b3c9dfa4c55388a128fbf62aa5927361":"3f552d45b61cf05ae2aa92668e89f3338a15ec7c5b7113b6571cfcd9e4c4a962043ccd9323f828dd645e8a91b007ce2112b7f978ad22ee9821698a4f2559d987ae4421452ad2e8d180953297156426d4540aff2104d8637b56b034a3a1823cf962bffbc465fe6148097975a8821ca7487e6e6c7ff4ee4de899fe67345676bb1c":112:"1e7dec83830183d56f443a16471d":"3d98cabca4afb7c1f6b8eeed521f4666ae252ac12d17ebf4a710b9a22d839b69458387ba4bbec2f6400e0cff80fbe4682c24efcd3b8c594d9b515ca7842c9d5988c42b59b6526c29a99256451e2927f5b956ef262f97c733dfa8bff73644473b9a8562bdfca748f4733ddce94a60024dfbfcde62fb3cbd7c3d955012d5338b91":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,112) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"d89f06eb07744d43d44734faf9751d07":"36cc3b2f563305208a03378f7dc036119f7de3fee77cefac06515853d36609a622382ed026c59783fbc0d9910767874c516e10c7bf3e3d104f73b3463c8d93a63418c76cb0d05e62e9c8642cb4f32caced2620912cb6c79e5110a27d5fba1ef3b4d0578077858526c5e4254365f2b2ab47a45df4af08980b3b7a9b66dff5b38c":"185f8d033713ee629e93561cf8d5acb8":"743bcb671d0aa1c547b5448d64d7c6b290777625ba28f25ca0fbf1fc66495a2fde0648a8db51039b0e7340d993aef8afb48269e660cb599837d1e46f72727762d887ee84c073d6136d1b0bc7d4c78f5673a4a6b73375937e8d54a47304845f38ca6b4f51cf14136a0826016535dc5ed003e38c3ac362b9d58ba8b555a05a1412":112:"fcad48076eb03ebe85c6d64f6357":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,104) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"6150f14dc53f391e815acfabed9f9e20":"fd8f337017e1b60d6618e6e4ad37c1f230cdeb78891579c2c63d4e6a4f7d2cb7252e99de333c73db45958808c08e91359c885a7385ab6f9ed98a27927a5b83c3a456ce2e01869712675e527155ba1e339ac14a3ccd7a4b87360902f2b8381308fe5a4eac5c90d0b84da4bf5b907de6ff3139cffd23b49a78750006100183032a":"7e92dd558bd2662c3a539dfe21a352cf":"9b4624e9118e6aa5dc65b69856638f77fd3f9f562046f50ba92a64e988258637932af7979f000505b84a71ff5dd7b60bad62586b1a8837a61c15a1a1ba7f06668272c28169915d7f06297b6c2a96c8c44203a422bfd25500c82e11274ffe07706365bfd3da34af4c4dd8ad7b620de7284a5af729bea9c4ed2631bdcba2ebdb7d":104:"922a7b48ad5bf61e6d70751cfe":"f272a3ee9b981f97785cc6fad350e516d72d402dae0d8a531c064ec64598b2a5760f9b279c10aa1ff71bec07300ab0373187138e7a103fc4130105afa6b6346f3d368b40d6f542375de97878ad4d976d64c5c4968a17be2b1757a17c03100231c34721250cd37cc596678764083ade89ae3b1a2151ff9151edcd7ba0eb8a4649":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,104) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"3e8216072ed6fcde0fe0f636b27ed718":"3b50f2a8dca9f70178503d861d9e37f5edfafc80ee023bfed390a477372986e4794175ec22ac038c3461aba50c9b2379cab48512946efdfe2cb9c12a858b373a5309324f410e6a05e88ba892759dbee6e486dc9665f66cb5950ea7e71317fa94abbebd67a3948746a998173fbbb4f14f9effbdf66d3b6e346053496a4b1934ce":"23a122cf363c3117b8c663388c760ee4":"28ce0b4a44fa83323e060f3ff6436b8829d4f842090296bdc952b6d4a6b1b1a66be06168c63c4643e6ac186f7ffd8d144f603b2d4bc0d65be48121676f9fa1f359029c512bebfd75075ff357bc55f20fc76d9f2477c9930f16408f9f09c5ae86efa2529d2f1449ceeb635b83ca13662860ef9ac04a3d8ab4605eccd2d9ae5a71":104:"531a65cc5dfeca671cc64078d1":"FAIL":0

AES-GCM NIST Validation (AES-128,128,1024,1024,104) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"1af434b73a1210b08595ffa686079832":"13f6c1c2d4edcf1438a7b4e85bcd1c84a989831a64d205e7854fce8817ddfceab67d10506ccf6ed9ce50080ef809e28e46cba7b0c96be6a811f59cd09cb3b7b3fe5073ee6763f40aee61e3e65356093f97deef5a8721d995e71db27a51f60a50e34ac3348852c445188cfc64337455f317f87535d465c6f96006f4079396eba3":"ae318f3cb881d1680f6afbf6713a9a2f":"3763c9241be0d9d9a9e46e64b12e107d16cca267ff87844c2325af910cc9a485c7015d95bbe62398864d079fb2b577ba0cfad923c24fa30691ad7d767d651eed4a33d0be8f06fed43f58b2e0bb04959f10b9e8e73bd80d3a6a8c8ce637bfbdb9d02c2b0a3dd8317c4997822031a35d34b3b61819b425c10c64e839b29874ddfb":104:"2ae7350dd3d1909a73f8d64255":"3cd2a770300ce4c85740666640936a0fe48888788702fc37e7a8296adb40b862ec799f257a16821adaa7315bd31e8dec60e4a8faeb8ba2ee606340f0219a6440e9c1d3168425e58fac02e8a88865f30649913d988353ab81f42a5ad43f960055f0877acda20f493208c2c40754fbf4ccee040975aa358ea3fe62cbd028c1611a":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,96) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"04036d2f5273c6ff5b8364aa595359c9":"acf79b6099490af938fb5fd8913255b3daa22786b03356cdf3e0ffaf570f9f866047b8e15c9953f893d97e7098265297396868ebc383be8547e8ec9d974b6a65b5dc5147cdadef2e2ad96696e84e44f364c2ba18c8aabe21f99489957b2b5484bf3fb4fecaf5ddaa1d373e910059c978918a3d01b955de2adb475914bf2c2067":"edc433c381140dff929d9df9f62f4cb6":"404acfeeea342aeea8c8b7449af9e20ddf5b85dc7770d2144a4dd05959613d04d0cfece5a21cbb1a9175ddc9443ffacd2085332eb4c337a12a7bb294c95960e7c0bde4b8ab30a91e50267bbd0b8d2a4ed381409ea2e4c84f9a2070a793ce3c90ea8a4b140651b452

674f85d5b76d0055df115608bf3a3c60996108023ebabe65":96:"71f818f1a2b789fabbda8ec1":"4729cb642304de928b9dca32bb3d7b7836dd3973bbccf3f013c8ff4b59eca56f5d34d1b8f030a7b581b2f8fdc1e22b76a4cbc10095559876736d318d6c96c5c64cbd9fbd1d8eb4df38a2d56640d67d490d03acc1cd32d3f377eb1907bbd600f21d740b578080ba9c6ddc7dc6c50cdcee41fec51499cb944713c0961fc64f5a70":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,96) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"59fe44c6e28d025b2ad05e6e867051ab":"20e66bae1215de9a87a0b878d39015d17e0d4542a1aaba2000cefbd5f892c26a410f55f0d7dc2f6b66690f2997032985e5516e068bfc6ec8a3669f566e280b0cefded519023b735ee3bcbfc5b6ce8203b727933a750f9bd515ec448c1f3a030aa0f40e607727a3239ebbe655d46b38a3d867e481ccf0fadbf0d59b665d2ed6b5":"eb0c30320029433f66d29b3fd5c6563b":"49b7418b87374b462d25309b1c06e3132a3c8f4a4fcf29fed58e0902509426be712639db21c076df7b83dcfcc2c2c8fcc88576f4622a4366eb42f84ebf760e3eb22b14f8b5ff83f06a6f04a924eaab05b912e126e80da22461abf7f1925fd72ebdf2aea335a044726e7c2ebbb2b8aeebab4f7de5e186b50f275b700794d895d8":96:"296c4cdaeb94beb2847dc53d":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,96) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"c314264cee0e6db30ebe9b2f6d4991b2":"d436ff9abfb044a332c4e009b591719a67b12a5366da0a66edf19605c34daa37588e15dd3da0d1a097215e469439de79cca74e04cd4904e5b4a6cb4e0ea54e6ba4e624ed6bd48be32d1ef68ffea1639a14e91a5914c2346ea526df95cbd4ad1b8ee842da210b35b6315c3075ecc267d51643c4b39202d0ad793cbb0045ebdc19":"4cd4431bb6dea8eb18ae74e4c35a6698":"0eeafbfd04f9a0ea18e5bdc688c7df27183f346187e9574b61222006f2b3e12e8d9d9bf1f0f15949ee1a7ee8e5c80ee903b8ba2860e15ccb999929f280200b159c2adca481748d0632a7b40601c45055f8cb5126148e6cbab2c76f543537ab54eb276188343cea3c4ab0d7b65b8754e55cfe3f6a5c41b6ea3c08b81fcecc968a":96:"fda18d2f795d900f057fe872":"cb9e0fb0ac13ca730b79e34745584b362d0716c344e4de90d8352b21117471ba12c97f193150b33774baee5e4a0f11b10428eaf0106c958e16aa46c5f6f3d99eed93d1b9ba3957bed05a8b9cc8c5511cf813a66dc7d773cb735b0523d8d6b0b80639b031ddc375f714c6dd50055320cd7ed44a471c8d5645c938a9005d0b5050":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,64) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"26072018bd0bda524b5beb66a622c63e":"91c524b359dae3bc49117eebfa610672af1e7754054607317d4c417e7b1a68453f72d355468f825aeb7fde044b20049aed196ec6646cce1eeeccf06cb394286272b573220cdb846613ebc4683442dccc7a19ec86ef1ec971c115726584ae1f4008f94e47d1290d8b6b7a932cfe07165fd2b94e8f96d15f73bf72939c73f4bd11":"c783d6d3b8392160e3b68038b43cf1f4":"8ae7c809a9dc40a6732a7384e3c64abb359c1b09dcb752e5a6b584873e3890230c6fc572b9ad24d849766f849c73f060fc48f664c1af9e6707e223691b77e170966ed164e0cc25ede3fbc3541c480f75b71e7be88fe730d8b361ea2733c6f37e6a59621de6004e020894b51dfb525973d641efe8d5fd9077a0bbc9dc7933a5de":64:"edffe55c60235556":"FAIL":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,64) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"201751d3da98bd39ff4e5990a56cfea7":"2965af0bde3565a00e61cebbfe0b51b5b5ee98dbbfff7b1b5bf61da5ba537e6f4cf5fa07d2b20e518232c4961e6bc3ae247b797429da5d7eee2fc675b07066ac2e670261c6e9a91d920c7076101d86d5ef422b58e74bdc1e0b1d58298d3ee0f510ee3a3f63a3bbc24a55be556e465c20525dd100e33815c2a128ac89574884c1":"6172468634bf4e5dda96f67d433062d7":"ae2d770f4070

6e1eaa36e087b0093ec11ed58afbde4695794745e7523be0a1e4e54daade393f68ba770956d1cfb267b083431851d713
249ffe4b61227f1784769ce8c9127f54271526d54181513aca69dc013b2dfb4a5277f4798b1ff674bca79b3dec4a7a27fc
f2905ae0ce03f727c315662cd906e57aa557d1023cce2acd84":64:"66c247e5ad4e1d6a":"efd064d4b4ef4c37b48ddf2fa
6f5facc5e9cc4c3255b23a1e3765fabb5a339fa0eda754a5381b72989fc1323ff9a6bbaecd904eb4835e5a511b92292757
4673061ed8de23299ea1456054e7ebb62869878c34fb95e48c8385b5ebceecb962654cf1586b3f54e7887ce31850363e
9a22be9e6fbc22e694db81aa055490495dbf2":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,64) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"3bc0dcb5261a641a08e6cb00d23e4deb":"d533ad89a1a57
8db330c01b4e04d08238b020e36aebe87cf2b0bf0b01f1ce4197be8b0596e475a95946918152e8b334ba89f60486c31f
0bd8773ca4ff1319fe92197088b131e728d64405441c4fb5466641f0b8682e6cb371f8a8936140b16677f6def8b3dd9cb
f47a73f553f1dca4320ad76f387e92f910f9434543f0df0626":"16fa19f69fceed9e97173207158755a5":"92ddd3b98f08
fc8538f6106f6434a1efa0a7441cc7f6fd0841103c2e4dd181ea0c9a4811b3cb1bad1986a44d8addabc02dd6980daf7d60
405b38dadc836bb1d0620ceab84e0134aca7c30f9f9490436b27acfd7052f9d7f0379b8e7116571017add46b9976f4b41
431d47bae6f5f34dc42410793bc26c84bfe84fb53ae138c85":64:"f5289e1204ace3b2":"be0c30deeffbe5170624792813
2002b24d29272eee6b9d618483868e67280236632fa1ae06f3ef793f67bd01b1b01f70a827367c1cd28f778910457c7cb
d977dfefff1f84a522247e19b2fd01fa22ce67cef9503d45c80a5084741f04108f2462b7cdd06a8f1f044fea2b05e920bcc
061fbc6910175d732f45102a63c76ae48c":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,32) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"239c15492d6deec979e79236baca4635":"d64886ce5f5b4
adb7fe8f95904bc1461749c931655b02819ffdd0ae31bad4175125aa68962f8e36ec834a7d53a191a74c937e81ec93ad9
ce0d3b286d3c11ff1733c0b7780130768c120b1833933561cf07399ca49b912370ae34f0e49b9c8cb9920eddc6816ab2
ae261c6d7f70058a9b83a494026f249e58c4c613eefafe6974":"916b8b5417578fa83d2e9e9b8e2e7f6b":"b39eb732bc2
96c555cc9f00cf4caaf37d012329f344a6b74a873baf0d8dde9631f5e57b45b957d6aec0f7978e573dd78b43d459b7775
6037cd64d10d49966eb3a2a08d0f4d5e4f5dcb8713f4e4756acdf9925c5fc6120c477f6dffc59b0b47a3d5efd32b8c9052
b321bb9b5129e5c6a095d8de563601b34608456f58d7221f2d":32:"fc08cbbe":"95c169721ea007c3f292e4ec7562a42
6d9baa7d374fd82e1e48d1eaca93d891d5ffa9acf5e3bd82e713ac627141e26a8b654920baffab948401cc3c390d6eea9d
7b78c4fcb080b0aa9222e4d51bf201ccfd9328995831435e065d92ad37ee41c7c4366cc1efe15c07fc0470608866aeea9
6997772ecf926934c5d02efe05f250":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,32) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"db68a96e216b0dd9945f14b878487e03":"5634196a32d4
cbfa7a2f874a1e0f86287d2942090e0cc6a82bd5caf40136a27ddf524a17713ce4af04ca6cb640a7205cce4ac9cb2d0ab3
80d533e1e968089ea5740c0fcbfa51f2424008e0b89dc7b3396b224cfaed53b3ac0604879983d3e6e6d36053de4866f52
976890f72b8f4b9505e4ebdd04c0497048c3ce19336133ea4":"8a1a72e7bb740ec37ea4619c3007f8ae":"1b4f37190a5
9a4fff41d348798d1829031204fd7ac2a1be7b5ea385567e95e2ace25bf9e324488dd3ab8ce7f29d4c9a4f4b1a8a97f774
871ee825e2c17700128d3c55908d3b684a1f550fdb8b38149ff759c21debdd54e49d64d3e8aac803dfd81600464ed484
749bb993f89d4224b3d7d55c756b454466ff9fd609019ed5e83":32:"9251d3e3":"0c6bb3ee5de5cbb4b39d85d509bcac
b3dda63fa5089793653133988296 2e8dc54c285c8944768d12096d4a3c2b42ffa92603cee2da9b435ec52908fca6d38e
d74f898fe0ffa761f96038ff7dfeccc65bb841c3457b8de1e97d9bee82e2911602ee2dc555b33a227424dea86d610d37c4
47776295b412b412903ad2cede5170b6":0

AES-GCM
NIST Validation (AES-128,128,1024,1024,32) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"659b9e729d12f68b73fdc2f7260ab114":"fd0732a38224c3f16f58de3a7f333da2ecdb6eec92b469544a891966dd4f8fb64a711a793f1ef6a90e49765eacaccdd8cc438c2b57c51902d27a82ee4f24925a864a9513a74e734ddbf77204a99a3c0060fcfbaccae48fe509bc95c3d6e1b1592889c489801265715e6e4355a45357ce467c1caa2f1c3071bd3a9168a7d223e3":"459df18e2dfbd66d6ad04978432a6d97":"ee0b0b52a729c45b899cc924f46eb1908e55aaaeeaa0c4cdaacf57948a7993a6debd7b6cd7aa426dc3b3b6f56522ba3d5700a820b1697b8170bad9ca7caf1050f13d54fb1ddeb111086cb650e1c5f4a14b6a927205a83bf49f357576fd0f884a83b068154352076a6e36a5369436d2c8351f3e6bfec65b4816e3eb3f144ed7f9":32:"8e5a6a79":"FAIL":0

AES-GCM
Bad IV (AES-128,128,0,0,32) #0
depends_on:MBEDTLS_AES_C
gcm_bad_parameters:MBEDTLS_CIPHER_ID_AES:MBEDTLS_GCM_DECRYPT:"d0194b6ee68f0ed8adc4b22ed15dbf14":"":"":"":32:MBEDTLS_ERR_GCM_BAD_INPUT

AES-GCM Selftest
depends_on:MBEDTLS_AES_C
gcm_selftest:
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDUwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDYwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASA9qWoAUHr
nn+3kxyNrjPJk82WDLimW21RN51uxpobadv8YgGEDRdP+Ok+uRqQSUsA6ZXfF3iG
r2GjfQ3wMDH8o4GJMIGGMB0GA1UdDgQWBBSjovYaC/m6Li9Tp0V9iZRs9267QzBX
BgNVHSMEUDBOgBTXh06MAV9S4l4lG1TKOrKRBh4qn6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA0ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgcjZNFWJtlDmoPZbAxqsGczRYK0lfPgu6
g1H7pp0ce+wCIDj9BRZM2OB9EF0e+MDKGjyZGfvfrL6Ir47x/KrM6H8T
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDQwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDUwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQEdT0OFf5G
UcrgX2XllCyJzP94NZ464GsgB6psNLsDeL+j7AU+oJy7VLvW/lHh3ODgl08Z9bhq
LFBmNjnHbm8Qo4GJMIGGMB0GA1UdDgQWBBTXh06MAV9S4l4lG1TKOrKRBh4qnzBX
BgNVHSMEUDBOgBQox4F1NsZunlsduoGvzIgRSYfB36EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAzggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAIW++zqDZlLLUk/emePohdNOp5JO3wS9
XvkBJ6Wua7GBAiAdx+EKmdjVrwnzrQltTgnmSfGMXhKNYifK3uD83W3pcQ==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G

A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDMwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDQwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQUXDgcUVNT
9hovbZE5HL6rjOb7C55wEuWKThV/CcZ4rWrXx7VXHYdD/R3aDA7JSvYpm2sTok4i
sblDzhZM/GDNo4GJMIGGMB0GA1UdDgQWBBQox4F1NsZunlsduoGvzIgRSYfB3zBX
BgNVHSMEUDBOgBQApzZdtBdD3dLxouQpr/aDiVttd6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAyggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgAkiNhqFAZXSUWEDK91OZvQGdeZOtd6mC
+Wv3fGk3t28CIEKOwidkUTUaiPdZ4efmAr+CEeGzdq27ob2S+nqqHqgV
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDIwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDMwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQRDXDNIi1p
ereudhqwa2LslXgsxnB63Hu5y5lg+1WPruIYPzD/Ho0APveVdzFLVji19+bE4+tF
PYL1SpsN1WfWo4GJMIGGMB0GA1UdDgQWBBQApzZdtBdD3dLxouQpr/aDiVttdzBX
BgNVHSMEUDBOgBT5RCgQ0AlZTQbfFB2+6+w0XRvydaEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAxggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAOnd+7bAofkHVa4KFNjv3TCegw1lrhuM
8Of8wgvrTEGoAiEAsS8iKMpSfXH4D0egg4gLamE6akde965rDtySU+ve9lg=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDEwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDIwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQWHpv1i6lf
wvNPOP5ka6S0n55EvzoaYK6pbTXP6yMOW/4XZSPKx5Zoq4FMe0cKzGIIFL1rzj1V
2czYB+qvLhyio4GJMIGGMB0GA1UdDgQWBBT5RCgQ0AlZTQbfFB2+6+w0XRvydTBX
BgNVHSMEUDBOgBSh3uHkX5nj86yFEFwjscSWM40P+qEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAI7unGW/gr9tOc3i+dF5N815srgh+FrX
oj9Et74EcSpTAiBubv+vOH0DE0gmYI11HeAIgutWqqMIC72dZlwTF/Vi3g==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB3jCCAYWgAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDAwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQznn9zHHwL
GO8VR4W9V7vMlxCdoojzEOiX5Y6JtPtFOz866ueHY6zoN0/mJ6DnqnSXilJIUUeW
6eGfqmka7nxko4GRMIGOMB0GA1UdDgQWBBSh3uHkX5nj86yFEFwjscSWM40P+jBf
BgNVHSMEWDBWgBQlFYvU5WboI4fcdPoiQs8/fPHZraEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggkA/KCWhcqToHAw
DAYDVR0TBAUwAwEB/zAKBggqhkjOPQQDAgNHADBEAiBasbuinP+pJTU4oDCVD8zQ
1rJBDSOKIEyWu84/D6Hj6wIgVMPUoO01bPhzllAa/gW8Xk/daey09SBgN3AT9pWU
TDA=

-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIBpTCCAUugAwIBAgIJAPygloXKk6BwMAoGCCqGSM49BAMCMC8xCzAJBgNVBAYT
AlVLMREwDwYDVQQKDAhtYmVkIFRMUzENMAsGA1UEAwwEQ0EwMDAeFw0xNzA2MjIx
MTUwMzJaFw0yNzA2MjMxMTUwMzJaMC8xCzAJBgNVBAYTAlVLMREwDwYDVQQKDAht
YmVkIFRMUzENMAsGA1UEAwwEQ0EwMDBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IA
BFW41/qAwAPpy+Txdc7PKmzZsq9CPiujKU4vpF1ekXnGx2HP420QobwBVVWhkzRm
LwdboH2j65dcCKjQ7mv/dxKjUDBOMB0GA1UdDgQWBBQlFYvU5WboI4fcdPoiQs8/
fPHZrTAfBgNVHSMEGDAWgBQlFYvU5WboI4fcdPoiQs8/fPHZrTAMBgNVHRMEBTAD
AQH/MAoGCCqGSM49BAMCA0gAMEUCIQC7iRcVzwMyfVK5imirJ7MqJQ04euH4CLOt
IZ+SNfaERAIgSU0MWFDosVEIpg8YMqIHeF7Mg4ZyH6+fGazJgVLttUY=
-----END CERTIFICATE-----
-----BEGIN X509 CRL-----
MIIBgzCCAQoCAQEwCQYHKoZIzj0EATA+MQswCQYDVQQGEwJOTDERMA8GA1UEChMI
UG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EXDTMyMDMxMDEx
MDUxNVoXDTQyMDMwODExMDUxNVowKDASAgEKFw0xMzA5MjQxNjI4MzhaMBICARYX
DTE0MDEyMDEzNDMwNVqgcjBwMG4GA1UdIwRnMGWAFJ1tICRJAT8ry3i1Gbx+JMnb
+zZ8oUKkQDA+MQswCQYDVQQGEwJOTDERMA8GA1UEChMIUG9sYXJTU0wxHDAaBgNV
BAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0GCCQDBQ+J+YkPM6DAJBgcqhkjOPQQBA2gA
MGUCMQCmsvNsOQdbGpmzpeZlKU9lDP6yyWenrI/89swZYogE3cSPob4tOzeYg38i
or91IPgCMD7N/0Qz6Nq2IgBtZORLgsA0ltK+W6AOS+/EIhvGuXV8uguUyYknl4vb
+cE+lWxhCQ==
-----END X509 CRL-----
AES-GCM NIST Validation (AES-192,128,0,0,128) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"f8022b8988383d5cfd7d9e0e208146e7868d3d714fe85744":
"":"5fccd8cb551cfc9c20998da4cb981d49":"":"":128:"1b5c6c9a28f5edfa4cf99176b0f14077":0

AES-GCM NIST Validation (AES-192,128,0,0,128) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"a7d4456b8e16b82283b677bd8c4b1f56dc7f153b5cfa746f":"
":"081de4a3f71f5d6fdf7801ff6c667f7d":"":"":128:"90c2729c5ba04f8f5c73726c910640aa":0

AES-GCM NIST Validation (AES-192,128,0,0,128) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"5779b60b536b096c9348cd8dafb3451280791e319b7198c2":
"":"62f8e195bc79957ca8ce99a88ded1a02":"":"":128:"699d71bb63c668b533c357662f861513":0

AES-GCM NIST Validation (AES-192,128,0,0,120) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"966cfb078f695c8ad84ede2fb96fb89488fa271dd3b50346":"
":"4a7b709d45745d94c5433b01fc9d57fb":"":"":120:"4a9bd213420629a5f6e471650060e0":0

AES-GCM
NIST Validation (AES-192,128,0,0,120) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"cc69ed684af2c2bd2b3e2d2f9faf98acf8071a686c31e8e3":"":

"0bd4197e5ab294ab7ab1e6ec75db2ac0":"":"":120:"6632b618b4cab963dd671fd53d2075":0

AES-GCM NIST Validation (AES-192,128,0,0,120) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"99deafc5ec6155043b53a86d466c2b652d59b7274bb844ef":
"":"09d18e85e5ed38f51e04a724faf33a0e":"":"":120:"90bfade2f07f38b2192e24689b61cb":0

AES-GCM NIST Validation (AES-192,128,0,0,112) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"5c0c706a1fd48005e0fd0ed91b4d9f0028c500dccb28ca73":"
":"595716e15498454577d3581e94f5c77e":"":"":112:"8b10eacb1f127f4c58cbb8c3516c":0

AES-GCM NIST Validation (AES-192,128,0,0,112) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"ae8e125507ea16d5282fe8bac42d3cb4908b717f345e6a38":"
":"0a7f64edb8cd8052fcd5b92e20c0bc2d":"":"":112:"467a2c0ba1d24c414f758200b8a4":0

AES-GCM
NIST Validation (AES-192,128,0,0,112) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"02176a5a5d8cb8f5ccee3f66a22181765ce730751c135198":"
":"c19ed1f52f5ebbcf89ab1907b9ebc7f7":"":"":112:"6525beb5856d6f29105777e31457":0

AES-GCM NIST Validation (AES-192,128,0,0,104) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"4434d6bce3a33551733d7afe8cd477a79be8eeac19bc0a05":"
":"b0eafdf326886eaacb750dcf2c104abe":"":"":104:"ab9f7923a3b9228cb9ecd7f907":0

AES-GCM NIST Validation (AES-192,128,0,0,104) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"39994c2520a6196cc3f3e8c6e4833286ce37399e0379563b":
"":"dbf9c40266d95191d70739e932cd8572":"":"":104:"b29acaf5addd6b379315535375":0

AES-GCM NIST Validation (AES-192,128,0,0,104) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"1f27d054114a264b37ee1821a077773750cc79d28594f506":
"":"6739d43092620f44b57e65035ce14565":"":"":104:"25e0434a3660704eee4bb82962":0

AES-GCM
NIST Validation (AES-192,128,0,0,96) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"0e97d15f4992a6354e43944fd346da65ac1f0f1229189442":"
":"32a64e826b500d7e85f4c42a784f7c19":"":"":96:"da8f3e0a6f156ec260aa34fd":0

AES-GCM NIST Validation (AES-192,128,0,0,96) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"27504fc47a9e9a85eaded3782cb5b088359ea1c0abbf2730":"
":"c55c8dc3d6d2970c81659f2f87bf849d":"":"":96:"113e637538de291e2463abcf":0

AES-GCM NIST Validation (AES-192,128,0,0,96) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"d5fc67f73de736768e5c64c37459c5eec3d27f7e337c346c":"
":"2691432d3935d4ea8cb8f7c17bef3558":"":"":96:"c0af76d6f62430106ca54928":0

AES-GCM NIST Validation (AES-192,128,0,0,64) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"f28292ee2c54119511a67db0d2317433abaeccabfdd5d1f1":"
":"cf9331a1bb3851b2fc3aeed2d1a33eb8":"":"":64:"8e14b869a95eb12e":0

AES-GCM NIST Validation (AES-192,128,0,0,64)
#1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"2042f9244079736291ba7fe1f030cba99672a97ce361dc14":"
":"aadfa619bafb21b5c738b65d632bb8b2":"":"":64:"ad6f52f25aea1c55":0

AES-GCM NIST Validation (AES-192,128,0,0,64) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"d9b4eb00ac03fabb5304ac38414f7782cb0186436a4b9036":
"":"809939260117b759d8dac1a69c27c12a":"":"":64:"1f7d0b3104aae50b":0

AES-GCM NIST Validation (AES-192,128,0,0,32) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"b5128f4cf91d53b3a50e9b76b0b27da33cbd4b9349d89413":
"":"644909f5fbcd61d850e43fbef1fb454f":"":"":32:"2ddbf709":0

AES-GCM NIST Validation (AES-192,128,0,0,32) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"3ac7ab2ade7a8e397d66be6dc7671f19cd39ad65490f1712":"
":"d152359d765f41dd9cabf5c8f37cfd8a":"":"":32:"a6e4e30d":0

AES-GCM NIST Validation (AES-192,128,0,0,32) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"f9c2de7e3c74b7e318413a32892d4fd070de9882158bbc82":
"":"63410c83fa363a63fa78303b9994b6c6":"":"":32:"49c514ac":0

AES-GCM
NIST Validation (AES-192,128,0,1024,128) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"66ebdc2332276784a69b6bb137161210bac9f1d6a36d6a4c":
"":"647f41b60c6a579086ba8854d043495c":"da26eebd04c27bbe7fa7b54b87d3b7227f056dd9c085fabfcb59ec665a2
57c6de68fd2c1c51aad5e6188e02a56f70aac49ba489802247ca327de57ea3cfa87e72cae7dd82b50341a2133b03cd002
7216fcd94cf43ec8a48e1c04145b597924b37f7977db3ff23b8edc913357037d0fe02afe2bba6b91e27554edbfb77f51cc
41":"":128:"420b320c2d616a0b11a7605a84f88e26":0

AES-GCM NIST Validation (AES-192,128,0,1024,128) #1
depends_on:MBEDTLS_AES_C

gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"26b04d8427582b04318fefebac2a2298ec3ce61146f39a35":"
":"99f3449c8538414e7ab595b92a7e6e10":"edfc2aa8ed91cfc0e117fc9e2d1bfe843c7cf365a2b6cabd4259686cd7aede
9c7453623967a30ffbd52b30fc205208bb346ffc70584478f5f39a79d4971ed71cc3dd0200a89aef6aecda0a1f3a4bf292
9b7b9e141be0ddd3671f727e5e793ef085f52ecb77a266b9a02a2c700b63d8c43da0b569510285e98b530abcdbf7739d
":"":128:"091cfc38b248460eafb181ab58634a39":0

AES-GCM
NIST Validation (AES-192,128,0,1024,128) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"82c8197e6641d0832639e2b1d7691fbac79618b2f5db45bf":
"":"69e1a3e5eed54bedc941646e3ad25a6c":"d0fcb4f4d764efc0fb52c8108e61b67a1386f1a13c1761941cc9a28c6ad1
5e78474cd2a65ae9475d70d9c845f14bf4d2bd2bc46c29e507a347391829e0f24495b026f681c387b3e6aec8acfa5ecaf4
c3cfe796c22469478ee6744cf04a22e6aec82489f53109551f58cc6602933d1780b8b45b933f76a94ef652a8ce8bac2cc6
":"":128:"8e74343ae8cf1cdda4969c1a94aab5cc":0

AES-GCM NIST Validation (AES-192,128,0,1024,120) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"1a349ba960b2c8f49b7e5314911ba8de358f2e74ceddf126":"
":"f5998a62ec507c5fe5b280f9c57ac626":"78445eceecf2e6d2ecf2589fd24e854bed3aecc63aef934aec9aea93dca95d5
8629002a4ba91e9bf6d12e13f0a844977b3c2700645281db5de381adbccd34a84346a99f34889bd46c75b1956e21aa9f
87684af55d7fd0de6da07e856d9b791c0a45e9e37881092f6040a9ae9d87757142d3c9c7fc6f25db0e5b5d377865ec4da
":"":120:"4d7eab0a3719fa53e552b9e5a85bdd":0

AES-GCM
NIST Validation (AES-192,128,0,1024,120) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"019af03d23342f7916e329b6843161e566aa859402cb07ff":"
":"c5fd96765fcf6d51e23ac6d206744af0":"f9808af3403051a52b6652df03b6b37d90a471bc242c436cab6ba699139ea
ad16847665093798731b9969709287199233c5e77351c5e42b15453b4171237a6d16aee63773c8c0d736b3a8bf38ccf
922e561c456682fbc2c7161da3b89526d9de222351bbd04ecd4e8680f26d70fe57d577ea287b199be1bbb8b76328ddee
3d33":"":120:"fd36fafe4f5571fafb6ece59b77381":0

AES-GCM NIST Validation (AES-192,128,0,1024,120) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"fab39ad2946b2a343d76b1ccc1939cce7ae3cd7b6ea187bc":"
":"247bc71446489dd3495c4dee8a071c76":"cb2c06fa5aa54ad079741afc56dbed79061a02045b6c099d0ae2d7883b78
c5fe09636cc8a5dbba0c0c76ebfdb81217526afbbe04fa4b2b78f3357025930b0f9488369bf3aa088a2107bfb6c4ba714f
1c26d0380d647ada5852d2c539300a4779295412b202c3cb977a7b94c24c4dd2a891a2035f388257b84e5b31bdc895f
062":"":120:"65e1aad214f49881a067d8b372ab6d":0

AES-GCM
NIST Validation (AES-192,128,0,1024,112) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"57b52697f72ae2df6354410a69dc3c5f28b31e6617bd78c1":"
":"0d96720526491d196eca66457e3c9e71":"cbdfdb3cc73aed4297ff9aba76dd8ca4d8efe11b0f521fd7170f07461c788
5252874b2ff8fd05a3943ecdc824ffcef0396980ebbddc0a53c6c99086c14fc806d90d35347d45e556e9a55ecc3a9fd74c
8e5dbd19ed8b452eaeb673818ddc0695f56ddf3b139a3df378fcfe5b6ccfa358f5a5bcd1550f1d9d5f325f15f9dcd007f":"
":112:"f0c49960e60fb63edbb50bfebd98":0

AES-GCM NIST Validation (AES-192,128,0,1024,112) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"7bf69ed06271107e11fdf016edc4aafb0e2d2ac05bdbc46f":""
:"50e65aa338cfe856c80cbe1331b46abd":"a7cab4e1e56f4b9fccca08d3791560e4b6c7ceb40a10adec0536861c5c46fc
3fd06c0a8eb32c9f18c40463b0f06cd0053e615dfd7caeb2b353b08ad6da1f8a23ebddf16524d2eaed70d4d7e565412dc
c9598df7e107beb464b103cd8de9301cafe8b0420f0c156025d72b73d6e015ed2312535d35899aed73aa54374674d7f0
2":"":112:"d7fb9d78fede77981948eb013ea1":0

AES-GCM
NIST Validation (AES-192,128,0,1024,112) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"caa781bbed41d7a1c56d47673f74d4310a3bf8b1275031d6":
"":"7795dc04261d9433367f51c3b87bf18d":"f44d77bd541e02a737c693ff3ea0adc091fff1966a593524e68954a2d7d6
6a48199366a5a600331cf392965b5ebedbf949203975fa9db53b72586615975e8a7b84e0633c6cf69caf482dd72b26b0
a5687ec71667e7f6e5abea89c3d69d2dc42a242ef959e4039ba5b2d22a3e48424a431a77e816604769d13b7f892e2b33f
cd2":"":112:"386930ced9a46097c0d1f6e65c62":0

AES-GCM NIST Validation (AES-192,128,0,1024,104) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"1b268de4ff644cfa4361f8014656d5d4decbcf9cede8605c":""
:"4009bb00afad026cbad117c6047f4ed8":"140c5a93293598fab85b3948b53e0ba15438a0b948e91041a13104f0ad263
c8a10613e20e87ef261999a54d469ba6f1abe56ec3979623df8520a0476801987c15410ec24f5a9be72acfca71e8c5904
e2ea5f8b22b8cf404b9fd533aa37e33b3d4cf91599cbb3b85ecda4aebaa27ac0365df8312c399ba1767c47fe0923f2c53e
":"":104:"af36bcee7561cd7d0861085d55":0

AES-GCM
NIST Validation (AES-192,128,0,1024,104) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"c2843bd689ccbba60ce961b7dd50619a59234dad97567e39":
"":"55a68cbaa5755d8c67bf26f03c5863c6":"d7980ab86ceb9b66ab265b68e078deddf7ba084b8967c3227839e8f31cd
cfbbffa004953f3582ea9274dcf46e3ad7e7744a576dec37e0cb36fced2b2c2fcf4328f506302f5741e696ce25c49492e33
c6a0c8aed5af03cdc1a266352623c6a52a555ce906f684bfd597b5e37f60b5175a981088b9d8b8b5493e4fc1bfeca64f95
":"":104:"66cccb7d28d3fa70bce2900a84":0

AES-GCM NIST Validation (AES-192,128,0,1024,104) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"f451c5edf9849a390486dfecad437cb809c33d31f6898ba0":"
":"9e2dd52c04651ceea88caf4adfb2e8ee":"87b804d4a81dc203d67a92b4fdeab959c2056dcedb28d29f216f9172817bc
fb3d2256bc1c8aac23feb22b71f1fd02ea28cdf91785931750ba4865d672345b5001b1aade4f6acc7edb03758d2540e64
72aff50ab3ea61a0b9ff37ff7a87b91013b14867c3e43cb097a923e6d8ddb1f52e4bd940b60d500a4e35bfa91935065f26
":"":104:"e192a49f5f2b22fa39dcfa54c8":0

AES-GCM
NIST Validation (AES-192,128,0,1024,96) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"bd02ff8cb540ba572af3431597bdf3f23e61665f96a19b4f":""
:"7198af3f594a4f0597f45fb592edef50":"ef06de48bd34f362fdb425c6e35e37d0dfa1ea874df7d201b6a1c25b736c96e

3cc8ed0915807fb7ed759482ca701d28c08cbf955be244bf887df37394d1ca4d2e7eace0dc61c807b714f3161f9d7f554c9f87ad674849c136108cfd8f777997656489d3e993aad4a51b68616083876832b3085a5f8f154b83ea44702c70f2980":"":96:"43298281cd27a36e5cbac4b9":0

AES-GCM NIST Validation (AES-192,128,0,1024,96) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"9ecab4a4a9dda43477c993d6388387443c66ac253071c504":"":"9523b2722b927dc3afcc5f7dab2bf033":"fb84e38a84225c8ebb307df88325d020a5853bb05ac7a75ee38552c40c302d263181081b05918775cf9cd6905b9982b2ae9ef7993f28fd8714e878c9a4a8101c08e9f13581dcf4f16dabfcb9d3c471c0056805f51e67e9b75572639c3d6ce62d2f8abd64e1e66ffb292360c20155e4d528374a5a22d845340d6f1ac68d33040e":"":96:"696bb674e43cdc7d69346555":0

AES-GCM
NIST Validation (AES-192,128,0,1024,96) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"733df8c42cc2e70ac195615d4911ffbecbe2712230c5c292":"":"f76135eab5d42e82aedff3090a1ba606":"0c8aea747cacf2f0fdfaf368cf32b12dc49f5da9a29bee380d2d64035b73efb56fef13aa20c0b612d9615cefb94f26978fa0b371a47dd20051a1605b9f5e133b52dc514577c53319c9e2bd4ac7cdf37d56a9e715e27860a09d86cc21d0b9f0f302f6acf06f2ff00cc6c878dacb8bde51082f701314de7efd36a246f80f8a8fb6":"":96:"82e6d0c076c7d8ac0839fe18":0

AES-GCM NIST Validation (AES-192,128,0,1024,64) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"ba33c24c41bf9836607b6dd05e66a3d16298c897dd1d70ae":"":"4b30423df6de76dd684274afbea089d8":"71f5f6ee7bbd774fa691a3d7e0f694a6c8dfe8aaf9cd720e163ef6d5cd949c798f9e9c993adb6d64e7220aa0f17331bfa9a43b659be101726a80e5529e827c3e4b05cfb4d78db9952e58eebe64dfbc0d1baf20e7e48902215277a49ee953108526a70ee150eda85e6a0e49955f8c6323766ae10e13ecfdbe4815f4bb4ba43786":"":64:"73e80018235ded70":0

AES-GCM
NIST Validation (AES-192,128,0,1024,64) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"1711553980e3fc5c14c98611ddbdf426463f82c66df83a70":"":"3396bd96b83ba611ed22e12e8a5ec911":"9506f34c90611acd6ecea385a782a5739f88b4fd13b77570c4d7e0617283e7b21568e32c42ada1cf6aca1a2e2ba184d4101306ff21c9d03e0ffda4854773c26a88a5173d52960286c18753df17361bb7046d2884ee600f58775304f49cf4e782ac70cb00b3d9c345cfcb38e3880743034640bbcae83112543cd1622ebaedb221":"":64:"5d51a0868a2161a5":0

AES-GCM NIST Validation (AES-192,128,0,1024,64) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"5d69dbec7ebe80f2b5b8f61fdff1f4413f5f6624010fb795":"":"a2eb3ba50dd93fa375cf682db7b2bc7b":"a0f9c0de86b54d3c176ece3305463237e1f70be3c52e2ab1c773a9d27d6fc5dadf61ce7a3d10dba8730d12c306fca8952403983bf242fc1b6efaaa153ca446a07d16a70af4cb1aa4d4c0c93d646dc3a5630f5a610aa9e6eeb873f9a06d3234642bc86b03c596235ec03019e762458abe17d37409a18ca5b7e0e0088391dd3acb":"":64:"1a827855ee98d679":0

AES-GCM

NIST Validation (AES-192,128,0,1024,32) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"7aa732879f290aa442217212156920c69457b8ec41eab153":
"":"cb593221c59846dc82fc0d0cd04af3f0":"15d7ebf94985c34b72b6675d7346f0b05bdb8fd3a278555939d2999028e
4179e69352d398a5dd0e5b370bdd9cbd24d576b89709c98b6142f71f5b1ba224222afb67599fc58fe043d1a91d7ea95b
56dbd086db8e3a061b1bfc6e82dc9ac728174fd3669d65db62a06380a5f72c3d091b7a1b6998041d5501e9fba8bf91a7
d278c":"":32:"55b86d22":0

AES-GCM NIST Validation (AES-192,128,0,1024,32) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"961a3e78f6a75944455f9d9d0345e08f4669972f3d5c202c":"
":"ce43a19ac648e62ddc49d243fb34e29f":"393736558133078a0367b8248bc18c8352f92a9212e90318a5b63ad3c422
ccda7c181c565629acf4fc73b2de85bc9cf38310fe703a877b3e7d3b2d416aeb962f1027077232cfa39c5e5284a1b3232
64175546ddfb250ce693e2dc78a0479bd89a7ab44b63e504866d2ec6b5153cfd51f29a91cd4fa2b8e09878747ae53981
875":"":32:"ac701373":0

AES-GCM
NIST Validation (AES-192,128,0,1024,32) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"c4d492904becde4e46c2557ac833265c715bb57f18cd040d":
"":"df41b22b92d43a96a7504514b92e644f":"c4dd46ce3e486d89903482de247c1e7df05809a247302db3ca8457b93d
6886c0a3d1be40a90f6502ec58d0ddd715896cee37322d48ec3f0c3ad716f1bb679afdcc0e4c79e5e2e346702d349ec7b
391ef7eafde618bbadce5d14d22123de611c065780a4d05e928e87d12b749888d6004224c3e457aca0190bf1a7fba2453
680b":"":32:"7a259bda":0

AES-GCM NIST Validation (AES-192,128,1024,0,128) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"316660f013ced78a16701b35479ffb1f7c8c4e964c1b52b8":"
d262c15d08aea46f614c7f8f6a54631289e54ca97d698777388e137f431bb783601e7999e7af98775d7b87ce061d9ba56
570ed8c58b6bbac5f12f751fc376ab0f14b36b40b2b5533727be3bbc9a51183405d5fd0121201ff592817d06613b504a3
440b0e1a57e9ed1771766a9a5b789054f7032d20b23c5c37d77f293c677fd8":"919ceb172d2cb460bdb3b3e58debe889
":"":"5f5128f7f948f0cc9fb248a24b07c54247e40080a992acddb2615d90ef9328a17bd5e9a698b00103855738aea55c4
944cde4a9148bfa8db12233231861c455e52c9889119ca402eabc8f41b27000156dd29b901024336cb2b7088eb5fd534
ba58f23caf140a8b2549486074e4edbfc262ed9c7c7ccaae24be8de873ad43cd13e":128:"ae22ec4c19e7616a5b877f168
febd202":0

AES-GCM
NIST Validation (AES-192,128,1024,0,128) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"1bdb707c328304809bf0608874c9db373df3c7104a5a7049":
"ca243caa145124997f5e2e6bb25d021a38d58d0ab1bbf06d086c2416c08e3512aa887cc215fdb34d0f2d78f6a4588576
7f15fc00b68a4df1130587de777efb9cfd59cafa077477e97edabf2bf04c9a6ce029c230385ca5f9928bca7fe5503b18774
849199d2a39a378a2d3144aef4416c1718319ff1bed8021dd77a07f61eaa6":"b7e7fc0d5adaed1632c5f7d1f56458f1":"
":"91c7954bdd6a49360fdce11c1bc710512bf5a57bcef241fb63e5ceabcdc9699d0c0ddb025c75195ec25e631507f13e1
8799e6be9798e5639ad8401f6244c5b0ace3905ae0de08e2d0fcd19d193de83943fe449af4b503a454c248e677d2f5110
0fd9b8b7e5388d5091089369a7c2ff38bd353e9757ef873a87f15f30232bafb4":128:"72337bdb2bfdd1f1ebe0dba6f9b7
b649":0

AES-GCM
NIST Validation (AES-192,128,1024,0,128) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"a6dd0d7e9d6ad1ad7c7394d53e9e081c436d34c8158bbc95":
"2d95d64ed3be857a5c79c7af20aee00f142557e10d780383fef2d45f16c7e2823ffee495b220c87971610e5650f7c3e8d
296b3f03fc883c00351df48d97717427101aa0c08a23c408b24511621b640c210b316cf17e3dfd714f0c9aa9ddd974692
d1c2ae27b9bb0fbb428e7a9da3b3cf9bd869e730ccaa3aa4bd08f01f84039a":"60b4b9c77d01232c5d3d4af81becb0dc":
"":"4494460ee73d3513814e1f779bfe3a229b49348d7641e9ed4dd959b582960097ef08b91292bb9db87b4e728d01b9
2683f4cdc81151a69bed2096bf6fb2e45d0148404420ea16b631b421e6f4c6665fe33c2d11e7b22b6aa82b610b83214ae
4d17e681972e3a1f77306d3c54d96c47d8be1fb2c8cae8300ac9db99013f25a65a1":128:"d40a246c18518ea9f8d733b4
2181123c":0

AES-GCM NIST Validation (AES-192,128,1024,0,120)
#0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"e9ed78cb5c10df05ad00c6f1fb35b4d28e6ddfcc16456807":"
e465e57cbac0dcd1e8ccda22042abecd9d89c4ac91b0e82a41fd51107a792099e63f7cf23a889d8c04edae2c2b3a9e51d
bee6c3b71ace3de08ab354a295888bb99ae0fe428dd69bc013d49a70511ef60524282347787a542fe9501b6452b5faad2
f129a9795c2c4cc0881ec4af8f0e0d2d4a7a628cb051055fe831b51e250608":"3a8ad989c621ae1e82b8d255a3c95028"
:"":"6855e4702f1ea593bfe30ee65b3fab832778d6b11a0ad902dd37361b8d85ab76d1f2ccf7927d695eb3129286c2673
7b9573e26bf64b31de26f97525f84345f73bda2888a1f53c9b405ad627bbe5dea123c9fb0a4b7f193cd8fbc8fa4a5e5f64
e9c083f5c048d61fd1d347b49afdc69e0ca6a82e3b064c49d5bffa2800b5cfcdf":120:"9661f5c3b0d99d4f762bdcabd48
df2":0

AES-GCM NIST Validation (AES-192,128,1024,0,120) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"76a5bc9a8d7c6e2822456156cea7d493702d61e7d504e3c3":
"0a7fbca875fd620c3d8de788e5c27534160f68d60d70fa4167adf0c18ea25fa1f2cc551fdf447aa16678d3f82193cf421a
6fa953532a3765bcb54183bf0e96527ae5e695ed3bba5d9911f36c1aa73132cd43b2698996eb43ff84420e315a06d7db0
2aee815461892c7ab9026953c4bc25f47153d5cb7b966b71b24dad69fa565":"09b681de6683751300c2ada84a214d02
":"":"dd66e08fc500426feb497c39c5853b26376272dfabb82ab5978167faa91adb025a6ca0e8fe3d04a0d97062eee8ca6
530c3788bebe4436ecdd3d9eab96d38a0cf9b8cc6a584a0facaea33ec2f4a6e61f780c3dad524df902f421e3204cec7c9a
4bb3f0860e017eddeb939cdfbe6f924e1eebfbbf8ec63c55b62137d9f8845f38f":120:"4acc40a4882d7733d8f526365f2
560":0

AES-GCM
NIST Validation (AES-192,128,1024,0,120) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"f5cb564cdd6974219e87f93a030fdcad35313d4adf9d7a97":"
210a799d480b4933e16fcbed632579beb6b00aec74c205dbaf64e2cb152c12f9b6969122f296efcfe328f542024465140
66594848f42a3031425020b56d065d6eaf2caf507d5f51df493c11514400b889f33d0b996e721eb613569396df0528aa1
4eaed117dbb7c01d9c3ac39507e42a158413dab80aa687772475105eabcbbf":"90f91da5239640a70eec60d849d9ae70
":"":"69a3dcf5b94a507a53fa5e62cfca269453623ccd3a537d971130a21bee884cf271b9833dec19862ab0dfe7052e7dc
07b20f34aac42bc39bf1d495360c1d701ea53a9bba64b02962b4ef64fb1c90a1a2f3a6f81a6ba781d5f28b786efc365ec6
a35c826544aab94b53b96613fddb65660dd336acc34a217960f6c22b9fe60dde1":120:"b67495a863fffcc773021dc786
5304":0

AES-GCM

NIST Validation (AES-192,128,1024,0,112) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"dc2c5a020d3ea731362c29d559cb14aa4f8e3f6a554a5fee":"8cf098cb6ad79e0f0eb4ca888da004dfe6431b5982bf1490c5f2d1486c288b5d50ea0a5a63cf9d097a71348632391b4bf962bf464419c2c971e76c03eedd09d069a070c86837e16a2c39a2cb8de3e2d3f274e03998a874fa98de0933b0856e076e7f575f351d7ecd024753781f51ef600405b304e37f326846b84692448d3f2f":"bd4d45d970085e0b2bfc9477f5cd0244":"":"d44a4fd303e657670632da8dddb6a117f3e35d8afce245e7e6576711c663f36806b813ba6421ef9788681d9717a36d3eff4ae1789c242f686d8cf4ae81165191220e338bf204744c9fc70560683ec07c212846d257d924d5fc43a3d4297ac54428a32c8bb9d5137e0f4aaa42df8dec37793f3965ca658f22c866e259c80bcc59":112:"9c1d6c70e1457a8d67f81cb3dc8e":0

AES-GCM
NIST Validation (AES-192,128,1024,0,112) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"167cb184ab6ad15be36536f505ea5447fd996b1d9a092ef3":"0b6ec08685b5a9d32346a5fa25d208136433204f3b86182bd1d9578f0634dcbb5b59937fb87df0679334d7f41eb8bec60ae1b87994ed2cfddcb56e95a6fb4e3ab7845b0294e4afa5ad46eb5a431cbd7ad0eb0473c42c06f3f62de03d10ddda449d41137c8010af5c7c0eac7a5fde5a39b5437a2382639fe3388ce029a7d4465c":"b5cc89a1c10329bb417e6b519091cee4":"":"7ebe4a9547fb115b39b09880d6f36f8cd402bb798c6d9db036b1ebd8b87a8e9d56fc23b7ae4e8cac3500bf2f73952c37a068f1e472369b62319a8b1bc085a51fbe47e1c321dd1ba2a40692ecd68762a63467d5ecad66a3d720a8a81e02dac0ebe8df867e2f7afa367aa2688ca73565e55cf2b0072fa3681750d61e8e60275aad":112:"30454dae78f14b9616b57fdc81ba":0

AES-GCM NIST Validation (AES-192,128,1024,0,112) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"9bc7aad4f4bd73acf756311ff1b72b41631344b9b57cf447":"7cdf07e17f667227edc986827d55bb803c6e51f93e72d98a1cbd161b58155a1c14ca54d52254e5f88f2a08614df68cc37f6e9fac88895b53090f69544b18aee4cc03763d35e7dd94ed82d1435316e7e02367b1c43506b3ccd31e248dce81fe62fdaea3a0bfba03477d5c151b0f76f09799048d8b23699d000a9da11281efffc1":"ffa8e719f29139d12f741f0228e11dfe":"":"6ab304cb9d1ed675383ff95f7f61ffc2aa73ab1b9a691bb84777b14c7014e986ffb91da6847d3abc0349a7aa09ed1d86f2dabc09e0e25a05800bd5d616c1a665bdb119ef71bae065ed019aed20ad3b13262a902f24ccb4819dc71419994a8b4774a3b9f4f672d31aaec997cfe340d2abdc3958c41373d0315076d22189eb5065":112:"260cce7d5ed6a8666c9feaad7058":0

AES-GCM
NIST Validation (AES-192,128,1024,0,104) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"5bd47bea08eab8694defc2b66e60da1be40fc1e398224f9b":"083ad3fe9273b8063e144a03f88fb179b18327aba37259d7f8532303306ac9d18cfcb746cab3f9385b5bb685fbc4a252dda268044642f5dbe33ea6e1634445311e440c5507fa6beaed343c83aeb0ffc4f1cba21b39f0ff6edfff961aed3ae1796f8bfeebcd3392d92e26dd26a19a7b7c2e5910f22557fad600f8cca8aba988d4":"e45a52c5e5ecc87b4320864b38683777":"":"8fa3cd91fb93a346e1f9595088c5503a840c7d7c33aa1be147e484e2aef2a8bda77275348ca59810abef6e179888f6781862990ba8e6d96af70febd2f671a3a8d6dce9be46c1cc6dbfaae35c35a7073205411cc8ab4ddd266b31b64edab4ffea076b29803149850cca41c857b05c10148182f8e7252e67069e7517da5fc08ee1":104:"9fa3372199a2484f82c330093f":0

AES-GCM
NIST Validation (AES-192,128,1024,0,104) #1
depends_on:MBEDTLS_AES_C

gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"850a811ca18044dee4487729e619cca71f05a5b164dd1250":"6ee76712d0b1fc00e43c2312743a881ed95a0b06276c5a4d93e3d56732af6b12c7c0d1aa6ffaec562229b6443e576caecffeadd9a65b91efa1bfe48ab1ecc63c381d00fe8dc7f11365f2b28945e844e7c6ca60972f733a96f29cc12e259c7cf29e2c7bbf8f572e158782a46093c5754656d0f2e1e1ea2a0b315b5fa02dadf408":"6f79e0f62236790c89156c14bd9540a9":"":"eb1ebd78d7ac88e6f927e09fecf7feb1aa64d7435aae76cc917edd9e0624a96e945df67648c187e397954da7b0888005f7a0d05d09de424c1a0648b56707b90da4021d5a36175500337e7341d1a474fbaa94e56d7ea52155829eb6bb9d95457c138875f0738034924d59681e7c2dfffb7dc0959697468ea2b65a884c897208ab":104:"91c74a30e5bff5b2585ac7699e":0

AES-GCM
NIST Validation (AES-192,128,1024,0,104) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"91469828dafd30de415067236d5f49ea14e813637f1ee0c3":"e3aac00bd05ce3c9b87720db82104364c8ef6ef25d6f3c8bcf5f73f1a26f8619e831bf7bb28c4dcbac7013dc6282d07cc225bd969c582a26accd7cfffe878a3159a5ad3cb6c8b89131aada61e2960cc5431f4ef94394634e4c8b2938409bcd2e7668986c7c5cd2ed5f2c525fa0212996960ab842a43869ed430d3291799a2a1e":"cb5409aad9d227a3cf0e2c5f1031873e":"":"4aa82b1c81a911cbe84231ce7afb95188f2177b539fb77de68f3d4801a2bd09f5ee2f7e59b5d9e79be5f7a23f0612ae39d59259dabc8b1bf7dbd4adc0db520bf7e71b988fa96d6b4dfc76afdc22ea31f64c64388dd93b27518b3263b0a19007405fc08645350a69e863a97dd952c8d886b5e0f444a6e77a9ef7c7de54f405a04":104:"2a6b14c78bcb6e2718d8a28e42":0

AES-GCM NIST Validation (AES-192,128,1024,0,96) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"7b6907853b7d4c4a19468111d96c5de048200b5441b9411d":"3622ba252c067ce7d6cae1d1f5068e457a0cf93be01fdce6dc8652a53135d5ed445388679e3f388ee6a81220b19356b275878fbcc2a6751bee7e2a50adb7c430e4c8cae03e88465f97bcaeb151d4f0007bee6bb9864b33020717adc42d6f8a283a20f6b62ec79fb8060e3e5ecc1e91a2eaef57e9dabd3b3634236f12d4bff475":"a66ee64c15094be079084c89cb1739c1":"":"2b8c1490e13881ab3bac875cbdb86baabe7fa30445bcb39315d057171e80d02aa8471355e80ba891b26d80b375508ba2756162cc688578be313a50096d7cd6253a8094970898fb99cd2967e78a57d12b8b3e3c10502634bead5bfe2c9dad332fcbda0c1bca16fd5cac78ebcbc7f15aad8b28abf3ed74a245a8e7a85cfaa712ab":96:"e52af33988855d1a31158c78":0

AES-GCM
NIST Validation (AES-192,128,1024,0,96) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"fe63e247e8de838a197a9e937e34c0f5a0b282533d445015":"17c5d748b8596901e97df660ca94fc970f7ebb769aff88f60acc425f50ebfb6744c6d8778c226c5d63653d9388d3fa0d4d630f94d668f3478c89e2708501edb12307a9b2189576cbc79388d291354cb9a5d1eace4ca1d9f734fc78e55ecbf86338a31ebe583cace752e8bafd0a820384136963eb2d2f4eea7b2f69597737a1ca":"8e018305675c287f802f28fe56ae5c4b":"":"c3d34e2cf1c3ad629490d70a0fec1a63c88d025ffed46ff8f5d8c0879c166ad716b702682cd0a437bdaa03a9b2e69a32fb7259b0fa930ca7a344aea37886cc9850e44de0aa049b8bc300caee82e26b2a1e5ab45c4c7cc6a15f5f595199999a0cacaa59da1b2be2a204fe13005b92ce722a000228545ae8a61b2c667a386f431b":96:"d7a6a917a286d8edf1289183":0

AES-GCM
NIST Validation (AES-192,128,1024,0,96) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"c739dae83a5e64bd98ffaf68b5bcbcd0155d8109e9ff2518":"56dafc06b354e84ce3ce31b7f88193124ca7e7049272beb93fbedcb3ede8e017bdb9ee5d314ec5168443fe01258d9abc4c

4c27580f6299b20082b4ca87eb2589bedc459f132dfaefafffdd13f82e153a2165dcab9a9b6c10f1d0d13b127312a6f5f3d
65a73b8fd057f1d88038c5137254111f7aedf21af07a35e34cf4d2166d9":"d80ac4dacb0f1441839e2068013dde3f":"":"
9ae5107f4394c9050f8ca8ae6d1eb66099ccd0166f38e45c1cbc17b30e218fcf6015ac92dd7ab48bbb095a0523904c727
10a86e50518d6aade269c82bc5ecdfa729802441e09aeb939abb43f5960542ad87961e2141f967d12f7190b07de99811
b264dc62cb8f067872f84d21b661558ceeae4922900ffd76084e450650de79b":96:"6a180ed4f3a9d5739e559d00":0

AES-GCM
NIST Validation (AES-192,128,1024,0,64) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"4c23ed64375d42c3a402fdadd143336d2f6babf4d4ebc176":"
5541a219108ce3ce593cca8c6aa6504c84983a98851bf8610d71f79a38bdc21d5219266ad56e10ccba4898ea969815ed
0d6df75312d657631e1e22e46f727a499696399a0955d94942a641383cadebc5328da2ac75bf0db709000ba3277581e1
318cb5825ba112df3ea9c453ad04d03eb29d1715412cc03dbce6c8e380b36167":"daa6f68b3ce298310bcc2a7e0b2f9fe
c":"":"2a4e04101d4c822eba024dcea27d67eca7ba7f0ea6d5290ced9376049ae085ccae3ecb624c03eb5b2808982c88f0
a5c4363a7271610b674317bbdf1538776f1fa2454c249a1b0d6c3e64bd4a356ac2aa2fd601a83d4fa76291f3ef1a9bfc85
8cc0aea10cff34ab9eb55411efec2a82a90af3fc80f3d8e2b56181630230890acc":64:"d408209fabf82a35":0

AES-GCM NIST Validation (AES-192,128,1024,0,64) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"695dfde34f0af192faa50244ab95a6059e2e637e237eb60d":"
33ca2c61a04467ad2bbd2ba8144573f0c2504a4e9945fbae250385406ed1757adb70534bd6ed854f227d93eee57c73a3
14f5955208e1ba5af8cc1e8b5bb07cb63030e3ae5f0ad287536f49b576418bb1d2dec40562f6bdda59c373d6668aaa9b7
91285716325fccbda2180e33955c8be19d05e389820ed69258c9b93e3c82e96":"a6a57792b5a738286fb575b84eea2aa
a":"":"b2ce449fc806dfb93cd7c97c018c2ba7d702216ae29a530a8f22d07279c7570c6288fc01fa9915b42a6be7a7d956
9f71b8fc2411dd9747b5c9c7b5c0a592bcd7e8f4530ebaee37e9c7d48d7a56be7e2df1d91cecfd11bec09bbca7ce710694
2989594e791e00e23557c843acf5164f3863d90f606ad8328696f4ca51fd29346c":64:"050bd720de1b1350":0

AES-GCM
NIST Validation (AES-192,128,1024,0,64) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"1a89a516204837bc780ad9b26717e51ccf42591bf58c75c1":"
c72a1b8707522442b992cb21a7526dfd341e27a11e761f594abbfacc2ac26ea48523d0113e38adbfc06d4af8809cb6064
54467fd253ca442241e8921b906d6c007dd09e139e568194666d5da0b33c7ca67876856cf504e8dfab4a5b0a77cfb188
3d532ef7c70b35b0838882f144991c25a2331863eaaaa2059401f61378750e5":"a9b1ef7744075cd6cc024f8c7b3b0b6
e":"":"0ec50150590bb419df0d6c410edfc2f8805a602ff247e3b50881ad3efb598ed053d8dd1deff86460db0081c0eb3e
ffe9ea94564f74000166f08db24da6cfcba91a9ee1e98b8671db99edbe8fde11d0e898bb130e1b27358fc42be03fb3348a
f7de9376af495c0ec71aed56d680632195539b2d1d5bf804328d0928a44c9731ce":64:"6c9f55e67533828c":0

AES-GCM
NIST Validation (AES-192,128,1024,0,32) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"4107d51f7d6e24aa605959d5d46b4c7e1743b7d5e3ae07b6":
"e5074ffbaf5e771e12f9e7cc8e7701b970aa7897928681383ea0f91bce8200ec6782dc9618e065e142c4ef2f7019791e7
4edfe2040b08bdf328d7d9658e7473beab65359d35ed168a2bb39f3c3f59890353405a82f48e16d388eb8f2145ed9bff0
16e725791cabca913813e7485f387223711c1ad098ffa0f72f74a048ec17ea":"94a88f6872995b26da39efb5e3f93334":
"":"bf32a717c945e1e2fe91fd38f3c7084210a7966cb83235d28f701ebcae6b2042226e932e4601eb3ed4728ca32bf706
5fcdc98017dabcac23f0f80c65e92518db6c78bf4cd91f817b69f3c3a8891786d433f6c3c1a025c1d37bd1c587ba60040
85571245591d615906f5c18994f09a03f3eef180d7af34f00ecfe153d5ab73933":32:"8d43426d":0

AES-GCM
 NIST Validation (AES-192,128,1024,0,32) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"0fa6270a44c8d14937cc3ff4cc2d2c997254a42ca8a09eaf":"2252d1c4706cc46ad3e4f8c49a92cdc7d1af24deaf7b08ab7304ef804cfe261acc3a202bec0d8df42cc36a5a3ace9ed7a9465cdec3513d31de9ae7821f9444226439c8f98a9a7d99b36b91b1b00eac71080d7eb550209af5fb7b3f28d09f5060070da73a40456d60c0470773af95d16c0b33d0b5327d44188619b950590ea862":"b5f3fde841156bc408ec3de9ef3438fc":"":"4fcfc56fa722af32e804dee0f4b67f5fea542b381bc47c41451844c82e5427f6cd90c37e088dbaff722d8700a11d5dfb4282e565f32e055324e5069931c86b62feb2cdf82ca1f62aee02a70e4e274b2b957650a5cc772be86c1b1cfc41b01d20d9be8b05b9e3ff65413520789ca0f198fe00d83483a1d85aeb13094c9a827e7d":32:"1ae8f9c3":0

AES-GCM NIST Validation (AES-192,128,1024,0,32) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"104c18bd2a0641fd46c2d7590d60d6d8eea74a2758ed0f4d":"4434cf5d12d07614227cfc12716a8adfc651ffe5c6476cf4489afaa698d9d19947016bdbcb5b625773252745dfeaf9b10021a5b38f742ea8a0fc5f926c80cef6568ab8639cddcf8fee9678d45ad4937d6e6b054b65512f929e897ed5f965cd14cad939732c53a847bb2758d818d5d131977649db5b59a0c5ebac37db961f9d69":"2902faec60f754f0fbb1981aeba277ff":"":"1789524845a1e36322c44dd1e938ee5d0fe6df244b751f3023d5d64d40a72598d352d9d2faba68be4e035c258b68782273925a94527fcdb977a41c1e0a96f53119b5909b23b0327c820e8f6da049a5d144a98019c4953aafd481190117573869109c265012a42f76bb4c3353f6613ccbc40a4af2f9e148bf0a0324bb43337fb7":32:"d36d2d06":0

AES-GCM
 NIST Validation (AES-192,128,1024,1024,128) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"263451f187b6dcab9d8dc4364217a483dd80c1d75f24fcea":"5e236c282eb4646fbd16a95eff2b27873f625a7e919237d75989a8a112ea80ce8db0b4aeaf5da59c3b22649dabb584284ab9673ba7edef59043eb8e99763643941a4788e7cf11bad63e13c9ef08644044b76beef68928dac22975481da4afc723b3ab3b498189542cbdffbc3f467d190cd02e9b36b6981122aa80cfa3aa3561f":"6c4552b3a03152aa464e88fd5b14356d":"435453a304fcd3c4bd6ab90d6ed8c54e6d21f75b9e56c9d48030499b04f6754cff628c4c9216f7d8a0abed5b8b7ca128c099a7deab74ecfe2c4a494b30d74833f837d254aa00d75aa963ce9c041f1916eb63d673a4af3f88817c65d4c86f5a3c28a67de2aaf75f08d1b628af333e518a7e99d980571db608407d3f447563f2df":"12dea5ea9b54957c689c7c9c6a711e2880645109a4057fafe3b32727a60ee1e24f8450310d6b8402c26b307bb0bf3cb7c6407270d95590efb938e6d77359666b11a7a3833a7122697e959645d8e9d835e0bd39bdc30397115b4c348ea825c850c1e54a60a2522a6321e4b99fa2ad9215205628c595b07c6ffed939c779d23ab2":128:"585677e0f37ae13d886c38202c3860b7":0

AES-GCM
 NIST Validation (AES-192,128,1024,1024,128) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"dbcf735d7c8701f537090d3dcf914c741ed783c24bd8265b":"18eb70dff73341298ce33ff4049fa631f2c72c158fcdea55d1231c46c95ba4013012b713bc95ba25a2114d0380c297acd05c323696db466874083e18bf544dabffbc70be4649cfe7e8bf449aeb9789d6fa412a1adf57ce732702ab962561f9e1fa850733c97b8a4158786e8ccf32af0fc2b04907124e731ffaf3fa7eacaa64b2":"09ecced8460af635e46bc82450352be5":"cc5b8f82fce3797009fbd38dfad7055a5e2ac241363f6773191d0e534e2b4592a6805c191daad377245c414df8edc4d3d9ecd191a50cf9747dde65187484802e15797d7c7e1db49ea4e423e94d9ad3b99aea6bf2928ce6addfc00848550b4d2e466e85a282cc022c7c4469d2cb16151e81bf63df378e0c676036197d9470f42a":"8298f796428faffa6085e458f149675d6c6e2cdfbc7994ee6f19af40fe8926c28904fd5ac0b9bdbd2de3f1614500a3eab1f980f82ac23cae80f3e6ba71539d1723e9f3412df345536f7517d847aae79a83ee9ad5fe38d60c6618d870cb1f203a3e1847d14d8de5295209c0e05aa196fec0eab

8389e4eb66bdf3dd49d0800ffad":128:"e53ca266dd93def5bee5daf70c953dd2":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,128) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"5f8d84908a8b7f5e118482bb867102a244bcbf48b7229115":
"9cd2a4e2acbeea6a73b5bffc1191d8045f63f3a14aa762eb776f35518f72bde4f9c8decd61a9319e3dfca82e682910a43d
e2719451e1a32839b29b27c3eb1c8f6118512d6a19cf189e2d04cf4e22459397936d60f7551244387294a7994320546f
070e54f166cd7c243d13f3017b786f7df6a7fa4ece05a2fe49fc39e2225b92":"5ba986f5115d40c2cfe404007a1e2403":"
06f98d4807efecfc863309f3bc64b0f04e4c16c32675ff97a3295d5657d4443f6c8b0a394d3f942705bdc19c22b8ff58e9
b7c209b528b745fa0424d5898ef0e42e0909aa5ad0b01f8549e3674102ddaf4784f0ff8908cf9f9a25e7e4dd9af4da7bd1
3ae0cd87b6aaa6b132dc518f4a95af403e612edce63e1424dacf8e349372":"2f168fd1c819b159739a7cc783ecdb0ef963
9b7965918e343e2a55f196daf584f7f14bb6e42d37b504bfc2cc08c218c5b841b2d2abce05bbf15315f471e56f04f7d54d
6f1dc7b7a68b8bc7026a1441105015bcee2c39d83be35d25f0d514bd1ffe75411b32867ebf2d532a766f9bfce9e55ea3e
0240d2a3713ddc2ba790bad21":128:"7f121ea36b36449e1db85e8a91ab16f3":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,120) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"f6c3037a59e98a9a81094d65ca52752ad92f93bcfa671821":"
26647f8f4092f80fc19f81f029c354c582b582516e8e27e97d50866e8ff755f50a8ae6422f4e996f0cf50826a68c007a5b1
6fd59002d368ed3285bbd04f8f9a5a524243cb8d5b3ffa184ba7384771bfc508f2e93abd2a1e7170d694d35cc0ff7f247e
84ca8889efc820c3f6d9cd40afd56c5799972d7556c91cde50ac808652c":"43b4f15bbe525913a31a9adf23d1971e":"60
826c97f0a99b88e7aeab774a3f2278f9d35b6c1a5fce49d9389a421543c99f68797224535dca4d7040313340da7398222
0040a063b045843a14f5d38763f95bdd26ef818f6e5171c8d5b47f183589afd6acd36e59b9946c1edf038ae285f500171
e9850603cda36043c29860e75bfe03c21e0ef11a9aecc5d5c51bb2201d29":"e58df99cce5b2548cf39684df6a26b8f9b7
969168ff21c410bc40b763842ab3b30cbb3c82e0b420c8100da61c9037a9f112db9563a3d069cdf2997e7f4dbb0b5d79
b56f0e985cd8cb70355366f7afd211bd9909c48b142c6556326062d27f7f82d76b83c433f00f1716ebc95038cb57c550b
5810b77788c8bf1e686a8a14b610":120:"ba6aa6d68a560642c266bf4469eaac":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,120) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"8fd9b08232a1d3fbe319d0897c74098f75b3e801d10e183a":"
a677a13ae26b7a05cecfd153aaaea02ccb50db601221a3df545164bb5fe638f6ed276d4bd172b9e740a82a690aec4f18f4
f3a0afb80c9a32188958e1cb3651064f55ca1211647903f63013e46b46c7f4f95589012eb4ccd2451d8e8dacc3cd06628
1f1f0c71f69f1c49f3f94136a522fff0d02427e4bccab056e615ff6fde1d6":"304c759800b8e275dfcfd3e5e3c61a7e":"5d
2dffb00a25788548ff1b2c94745e5bfcc05eeb11e63501007335d4bd06bfb3223d4682e7e83eca0e163d1a8f2a76096ab
2839ad14b45eb59ea9b29feb76f40b0d8dac55247c65e5dbe6bb2d5155ddcf2b2f924c48e1c16c990b69ac48ef2350873
c1ed524ce1b8ef6c92a11c8e461303f7c32b5d65b57154197e45f1c6b792":"0779e5050dd17837d40fe3427322e717f0
74312f160c1951e5560797c13e4fbe47f320dc8053a39d2def4d3cc20e215978647d917ddf93fdf9eee5e54a974060dba
c2a478afe5f5acbf65af4dccbd3942d130dddfd90cfc969da0c7f4b4050e34ce2e049c3bb004782abf4744c9a3ca2713ebf
c5dfa16d011bc0b33d0368c108":120:"54c8a1dddfaa1cafbcc1883587b4cd":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,120) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"19d38467c1024611433a0b2780980538d88f3e8907a86e42":

"2623cd0eb46a7366877149ce0204d7dc08a5e64a1adb3b6759178c4eab26ca1806fc25fc0fc99dfc77d1811e61ac1e04
ee82eb69ef7527962df1707734e4aca970b8a499eb70c2b0386942906945abcd9234b92e7bec33009e70786c39bd241d
a3905d961473e50367cb7726df8da2662fb32101d13b75032838f01ad7946670":"8d56a9e4bed67a7eb0f7b8c5e6bbf0
4e":"1c7d2744a56f5185b9cdf14eb9776ffd315214540daffc69c217dd64c7d0fb4a9f7b1ccc4c1e325fc046eec4feb8df3
5d32f492a28d35858ad1e9bfaf95211f111473c2ff799a124b308fba996b08f185103607605922bad319c6b7fd211f97c8
61565bea34948bfd751e4ce2591ae777ab1df8dc9e820cdad13066ed74303c6":"edfdfa35b41c5642e5b4dd1769b6358
11a48ecf21915cbef3c9e2f8230953f2ed4fda8903ec7634f10d55aa58c975a6c6133a173c2aeb83d6d7fc6534ea1781df
c62408e7a17d255a983bd1c33d2f423c364893db8128a599cd037b2db318f86f1fbd895a64a9fb209490b7e9a30db8cdf
42e348cfcfa7984e15c17db810ec19":120:"17dff78f61d21de4c0744e57174f70":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,112) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"d69bdc9d35589e33ea9c2b956780cd9618e0df79d1083e69":
"d8a75de22fd3e2d50127c6fdeabc09fab1178875998319e1ea83c9745a1d5833c6ba9df08177c349dfa412e13e1927bb
d4cdfb54a21c86c149be1feb4d9de99ffd590850875a3d9c8d9306971a9802ad4ca48f73d0517322525ac8463e3d59ae9
895c9b363b6f0728d7585de78cbb49757bd1919ba2f2d6ba042d0781e7a79d7":"abd4b94362501b8f307fca076fccc60
d":"1ad9aa99a4c8158ec08d21ebfb62604a043fc0c248fe08daa15a89f4a7855916af8aeb681ac6600c0268ade231f918f
e508f48c9cfa998effc350fa117e2772f04839f8fa1a53bca00693ecd28db27c6507750404bd89af07451d66fb7dfa47065
e9d3fe24a910eb27911591e4f4e4746b35359afada4356676b3c7331c610ab":"52e88b54b410dbfb4d88092df52688ba
9502b906752b4802aca5428437d795de0d3539945bebdf2bab070df4a7e630469b92fe2dde0998d44094cae7f21f84ea
7806637fa5c73b138e87d04005ef1206ddf30a21f46c0aa718665e809ffc0b42b5250143604b20225ec460defaf554a8bf
b5f69ef4244e02e9563c374a44f0a9":112:"1024f8e9997f5fa4684930d17431":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,112) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"6960be8fe82061e9cd783cd1c03f63a00d60ce9fc47ea496":"
e0f574ddbb04831b5a86f40182f5f10d8667fe13c7065b471df157f67230c41b8c069c0218ceab93d63964be8ee853c56
7add2c3eab1670b03a51f9175e8e763be778ec43833cd716e1c8fe5cfb1d663149b21e06df772a3973fe1297d65188201
cdb0c3533f5e9d40bb0664a97db60fc99d7e48eedebf264024006ca36361ac":"672f4378862c82738055273c72555b39
":"e3a4dbce87edac519ce86349eed2dba0d371cef0d8f20b4dda3e1cd9f5799c9fd0b7494daec5bc995a6936c501212eb
957ccc9ddd4c9b8a205cac122ba87b5c5a0eeba6b2af2cbc2326d953d61d089b6334ce03257203072f8e06b8c6f37692
748a13e681082900fd32f0df6a3072f3a8b9bbeb3ea558e97a43d6656093d7c75":"2a3c4b79bbcfa4af04baa8413f6f1d
18c9c579060ecd0cc359fcdcfc0566697ff834f7dffec84b2292e8583ecb59c9e5e5d87913a6ccaacebf371f1fff67f0be74
9d4ea5f5c6f4c959e9d932414a54a8e25bf2f485ecce9e70990bbc4e621ce2c8fcc3caa66b0730c6639de1bfa0124afe351
912279bc3ca363f4e6013496cf1":112:"dbdd6af194f2578a0d0832d0cba1":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,112) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"2b7d0115612c56a1f28c6b3cb3d51c2b4bbd4cd36ccf3dda":"
3a88efa524a90b31873cba177a7e6e050dc59f42c934923db1e75fec924908370ad0c9c3b0b3c05adf12c6ef2627d8d16
f832071c055aef5f581a39a8e7d9bed2629e26d5e3ecaed24048d744fba08d8d12132def62059f1a549044c1db121f47f1
0b3dc4a02849150aef53bd259d6814162761cbc9e1a8731d82101696e32d4":"317a60c3c29440b8ba04daf980994c46
":"80d816bf4008ae51b9dd9a25c30cd7482f2289f5616c41d99881aa8f78b5efff84efe307a822174f3a5c08b381bc99b1
69b92057627f21dddc367723eaca2545ce3a4fba2b4633fd99459fb03e85d6d11ed041b63185f3b94f6004bdce556e2a0
aaf811faf0153b3974d0bae3eabadccfc95474c940ecad5b4d5ea88f88b8c4a":"f193303bb781164e42b3d4d25569a446

c86646bc0fbc93059603c0b46ec737ddfcd55df8c90e6d806bd9fef90f2b122a1758bef5c75fcdff95ce44217d9b6b0e75
e77656cc7f8a8cc47729c74faf43cbf08202e9ad16c7ef8c832ce5f97f51153e178ccc3c168928f3c328cd5b4c341bb048
2f6a292cfa2fa85e03d95bcd4cb1":112:"42308ffc76cb6ab3c770e06f78ba":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,104) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"75737e01a95c2ad9c860e72a57da646e01c2286a14dfec75":"
fa749799afcf2242a6000c4fe1e0628db53933dde99d672e3c7b24b0cd6533b8002bb7aa8633322f4ee2e343db3a0067a
d44edaa398cd90ebdb50c732e8bf95aceb4aaa4dfd1eaca617c30c30c1a18761a6d24c2de0790f54f73e0802eb82ffc012
4517ddafe8336f4ec6197219346deef4ce930e8ae20117e6ebe49a2582346":"1060d78543be384e7a9dc32a06bcd524":
"528a6c34c3cb3aba402b856dd7c9677d0d88821686edd86287e7484b72248f949bbdfb640df27e3d1d6b6dc1293ea6c
84be72c85e5ff497f5da74d796a21f2513385a177f29f2154b2362d5ac83c3897f368d06513333f2995b701fb3e5aabac5
59f6018fffd02cd6b65eba9cdc629067f15d1ae431d6a22811508cd913009f8":"7e8774cb73468ad9647f6946aea30e94
68fac3850b5ff173c7b346891ecda32a78b58df8d835328615f36a12c18370f3abcf021ed723830b08627767272f769a2
105e4786451db0512027ce0e3f770fbb0ee0e1850a5fc479df4ad5ceff4fa3b2b9124c330c2e79d770e6f5e89acdc8d0ca
9c758980dfefaaac41aaf6d472f8a":104:"6bc6632bb5b3296ede9e1c5fcd":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,104) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"a326226b24222b3389d793b61b723e9ac7059495a1b597f5":
"1cc26e453a54c94c1cf902fe12307cce2fba4d5f0fc3bb63cdbac0dd0b5ba31d08dae2b4f054c86f3a3ee920d8b9f7ad8a
e8b4eca090c8783cf35db5de3b95889a84f09ff3f70263c61681f00a454b0813813f0fe3ec38a6d30cc3c6a93c91a42274
3e7a72340cb012718b8a4a3b66a75f13e0165aa51ee4b00046cba12e966d":"327972d0c2ebc20ed5bdedc8a3a7aee5":"
2edb1455bf4573a54ab921d31b7fc9e534bce0870eb6e973afccc3b1f93dd2c1a476dd88e705919caeb5d4f4a8516a718
cff8858eb443ca7785579036cc7273570e7bf2489ce71a52ad623bf7223ce31232d8c9b18e52a2dd4519bb08d87301f3a
e69dcc36c6dcb3b03d8fc39b6621f6b4471092e941ef090c9821a05df8575a":"5a219a0d997e879ffeb548d43de8e4f32
a9ad196dc425c83f766134735ad2c9ff5d9665bd54ac3efdc50bb4a7a04ba59825f31a0f3e530aef45bba00cd6479efaa1
9c85edb4734f91fdad6686e50f9cc531fcabce9e8397381b4d691da4a27b7c487e93de3e3a9e769e831c69b07697e4bab
470ebff628e710efa17e4c184e0f":104:"2b9ac273c059865fab46f05ae3":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,104) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"cf5f2d843042ab94fc4519d57d9229ea7e8172acf515fab7":"0
e20f5a2afffa4a5f9219320716c8a26e35a19c525dddd528e5f5f06f0da082f43272361f07cfdf57423f67ad3cfdda9cf174
7c602a93747cc571adfabcc9d1ec1a8128908df45fe0ede0e14ff40169dd1ecbff7f4062ee7be0a1afb370c9d5103132c1f
bee9262309cb05ea150fa862d6303af71677d2de9cafdb4ecdab8d5b":"95b06c3ce1a3de73cf51e781b941097a":"765c3
fae74b6fa4b6ed4ca7ab9b829d76a7759c50874a38d2ecfddaca2365f7a143c9584e255608be829950393e5f94131caf4c
aa04aeeeb9d595e39ef3f9830246d6066995b2d40438f7eb0944bd452ab493b422e93a3e0dc3c0fc2a4b83711ac6693f0
7f035fd9d031242b6ea45beb259dc0203f497a77106392e4da93c285":"f43628a227dc852e0ad931e23548fedfd57020a
26638ceb95dc5601827a0691c44209d14113da56e6a1e44c72845e42ebbc7ffbbc1cf18c1d33ca459bf94b1393a472568
2f911f933e3fb21f2f8cd1ac48bc5afb6cb853a09e109dadcb740a98e5e7ec875cea90be16bcdfec5f7de176eeeb07a3768
b84b091c661f65e2b905e":104:"77964b5ce53209ee5307065d49":0

AES-GCM

NIST Validation (AES-192,128,1024,1024,96) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"11cf18bbbc1d8778faf40391c30ca417739ff8e2a521926c":"a2e11ac093ab648118759183cd52ca7d5728ca87fe2f31eca28cfb13325e3e6e95974456857866dda78359023e2c998d2c93c6dfe8f72c6d4ac39ca0585a53fc074bf1124c3ada92e78462a445da23e650bf52e26b782ff50312ee2beb7410e93c8435f7b88dfb0ed63d9a3823992d796bf3ab147c33593c5e6193ef32f7a620":"bdd9a2b70e4ee0cc501feca2a5209c3b":"051c68fe0cd81b52fede137d0105e69c74771b770ea9b573ad92ecae86f420953f459755597f68c29f6fca39a27239faa940ce6c949ccd44c9f12a0160cf74a575753310f52ec5c5bb9c4474b85266494e63b6810ddf7a6abd1cf8244cebbf69d3198c4a09e8dccbc9429f81791f5c02628e9477b988e2bd10f9bd5d6731ad01":"ca899a00654730d68219ca2ed9b23058a5f40150c237143b24245de1e440329e513690f00c0c52bbd0de8074fe5d7a50fe420470249227f967340efeeb64c424881c7f3a20c405d58ea81f2309c7f74ae572b30313e2d4b419fbf5f2cf90c6706a1ae1a800a883e8b00fbbc9dc28bf5aa4a329246bbe94df5c2d4524f57370d9":96:"dd45503cc20493ec61f54f01":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,96) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"812481f8982b42b2fb86297c4b7c739652908dc498171c69":"32b27127582ceac21f968f5418e24ec8b84617f4daab0eb007f02d45812e81d486dc50909d79221c438def535b8a55946f50297963139a6b21e139e810d19bc1566b374d080a387a646bb582dc738c44156eb6c8dad613586662418edcbb18fe688d271108318de71734cb571d442e4d9537b0fcb2f5c763b3fbcac010f5c4e1":"0dad658c73c9c88dd927a502d7b14e8b":"af44f747d77a83ef0944f3bac8e835d752bb55772a7fbd3c6af27ca0eaadd122c9af1e2a9f37c2ba42779ed8cde2199125378fc88c7d6d58edc01c65491c5efc6bee58e7e8bf72f1a69d3dba47b38a50077130cbd71accd3dd4f193a53c6f2d1df694476767f79f8b71fd42745ee5bd41e90a7dd50a1597445251b32de303169":"003ae4798f6a0b97990d41373623e528618f9299cebdb0d23e3799f62bb063e5530eef7fc40c06af16965ff6895f675ffb81c004d826cbd36b5eec9bd3d90d785af03b64d12d311b6f90bcd75a40497d0fad5e54f829a097b25f7a9604f6fad475c9239a0f8d5589b8a76c6f7bc852a3b820734b426f59ee845ec3f09dd7d3d1":96:"b80bbc002cbebfb4ec5d48c0":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,96) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"a6657a7a9ddc6b4595df94d7c6bee9d13ad231cdc46ae5b4":"36857eccb5b3c220265a40980e8949135e840ef270602940d3394f3f679aed55217c1de175f6b48a16f7b394ad7d288bc425762f971b752d1372b369fb1c3a64970c8d18ad6de2e1a9a561a749e3cf9a8524e239f3121e8643bebee471e55fb5d54a3453c51b1747defac98ead8b25854ed1cae7ac44fd28cf4b1ed8988875c1":"68621ea7c6aaf1e86a3b841df9c43aa8":"bc25c38d3a200fc17f620444e404f3b3999f51ed5b860c04186750f55cc53c6423c44d0eee02a83af27d16b9652a7cb3d34a5cb19694e5399a272dacd56c4b17872fd23fdca129a4299b9c87baf209dd1cd1f355088e3f938e6d5053a847b5913f0b9135d6f290e365508bed73c61160a11a2c23aaed7551b32882c79a807230":"de8bb8e69f9ff1322f0a6c30cba5a6fccd7d17a2173a86cff5478ac8ea4ad6f4e99ddd4149e6a9b24865cc8fd6394066e24a556f3f6d48c599592c56f06a946c6b3414e2fb47e14d1f128ef26b385912367f35082099c1f3d4ea86687f19f059c56dac21923e9a151567299416eb311f5bbf9a28968b080b0b200044668f0919":96:"065f6c2b86891c719ea76984":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,64) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"20cf8c2c47cd583286157b45b575d4d69c793b4250274fe4":"a64c2131c94fa827c3a510b23b20fb6d04579bc292d2ec33efc9eb31459115da143f73fba9bd8b03b67e591497d108f900a7279542b480bd3a13ea588a29efe66688b52c3fd58598c66d8595888e87b27734e6c5b2796cc60ab2aa3dd06a29c577de5bdbf0b6c69c7034f0181050f286b9300d214f549165a0b5b56ba8e40641":"ab58d2e18eb83c20df94cd6b569c65

fe":"93ff6057eaaa9559d87e3276d4d900888cb1f56434ce2677ee1486a0aa8f4e8d02c47d06e6841f3fbe5bd72dd37fa9
d81bbef807dca6961910844eb9611419936310d717e1843e7b278f48ae44a57c1f227a75fa8cbc7fd57c8cc3b101e036c
8ef3043642c81f381561b61da7c9d79b6da9ec46f7cf093c29c1930b27c14f991":"a3f621261af17ec475624541428001
7fd36133f2f9ff89eb8979d4417b8f93892bbf7b08bab785341bf0c7b5e3643f0e33f036633e5ebeae7a750ffdfcfbab690
291731e92238ba6b45859b309629224fa7efc72298d3cf1ae3b6a9e94797552afc4e3a46205f9bab7eb64e4a41aee0e45
289704a97221b7118d209e0b267a68":64:"ae53564271d5de5d":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,64) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"8a311bf356cb1d1f58eab411b45b8d78b88052f3c8ab821d":"
3e915e92f186fde05ad55a2597ceab81495abbaa0be107dbf6a375525d1157a322b1f65460dce0c3aa2bc08fa89f777dac
4d2fc3e5f7f20a0d5e33373c7f1c3551369737124c702928726bd9db96a33bacb56f1d645fa02ca1d88629c547c0eaf95
85ee23b530ea971bf439c67e3b752af882668ebe0c739b26c837887b9d2be":"0569d05f3825d16aaa89e86812f80628":
"28494a12026eb89b46b6139573dcda0836a617e00e25e2daa92f9372d86c3c162cfec34d634ea48294c784825615f41
e06e555cf916983931e3d6a7ccbb4448670139616e3bbf7109387a852703b0b9d12c1fbd966f72bf49a7e1461ca71487
2ccdc59dc775c24a85e9864461123710fd8dcc26815894ee8cf2ca48a4ec73b3b":"9ba776653e8d9d240d9c1ec355027
a18731c500928925e7c50ef83c6f36957073a8386ecbfaf430634cd557b1da1bf122f37456fea3e9b58a6e99413d9d16a
2f1b40dff843fe16a2fa0219ad5dd8ae4611de53d7aabbef7a87ce402e62276addc7f44e09ae9e62c5cce4ddce5695db98
7084385ae9a98884ec97e67b549ad440":64:"c669ca821b6ef584":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,64)
#2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"82fc47638cfb361ecf7924c03925d6006cb99459ef5691e8":"
d14a550d419b8e03762429a7abda3b17ad7a1305e5fc639e71538285cd70d78fa30e0c048e2c32d2a7fd7f82c874d63ae
922db5a77111b46caefbfe4feef4df19786e5fec6a4df84f76df412b1f06bea149f1996b41b117d00d422bba5566d3af528
9ca9377f325ca1e72f7d6a32df6607bde194cf4ac52c28e8aa1e8f1c9a67":"2a8e1cadd2f264f2ad7be9e7bdfa24a2":"80
88358d7c3ca8951d7e8cd6cae15844edabccc8d0fcf8f169a48cf434d4814f1d7d9ae410e5581d414f952f52b852eb10fc
f0f2a67bea826ea2e28331f0597152e624e148462d5952f10fa363666d57ebfe036695e1e68f79161b991e20c8ae60952
32e63fde073c79603135849c62f8d98a1d80608fc081171114db41883f6":"e54cc95e845f4d1b28885e9b90d1d9d3cc5
1fd9d8fec9bce57de8781a28b4e5b7ab446074e84471d7a9a23748b689c354e402be77f9890a9c52a2eb9022a6a415e0
1285db1c6eb66d5e15f4216a4f3f45782677b6ccbf20ac7b35bd153f52a599712d09712ef1454ccf72ee48cca967f4917f
1aeaeaa6eaaf8493ec7ff2dc1d4":64:"093343e49b70c938":0

AES-GCM NIST Validation (AES-192,128,1024,1024,32)
#0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"d3180703e1ec93b20d1ac4d64e85d5461d75f783bcd2f4fa":"
b7b350db6fc0796e9fd0cb239f561bf7e27b2aa26b8e3e76d8b737caa1c1c5ad624a32f5709e4b751f8c21172d4d0f4ba
38ca4d1d0e2570c084cabdd0e8880b35140c84f775c3c301a9b260825e1fd75f9835777d6c0e23d359af1a5f7caef934b
91bee521531582b639be2cca87c2991f5525f4a2f64c30a1453013d73c16cf":"916d72d515d3247ba48828d4113bda3b
":"1002513035cb1d7e8b2710ff8c93cec55e2e2c2b56000d4c1182b5286736acd2d6f2fc9b82f71156dba6f774638056
27e4bc38c96e091ecd945df7e996e7fc3bbfdae3d85ef1337fbce960fd1d60d06962a1669e9e8d20be151f6323cb38ef68
ab5e838f02a0f379567f518f15d81b192cb25a42356807c1b9c02bef8309ff44":"d590f2afcd64c574ece12c675f509efdf
fc01e1404cbafbc923c4b44390eff66dd839e6d800df67bc06f49f76911df3cec36a3a1521762d6d4a8ee602ebefde0178
863443f918668fcde8a531f3b5ee0e4c379ecf3e75e7c59f753e41f4e39811bd3e7dd3d6bbaa1e81fdbf8bd976384a6c45

05f7e4270321c7329bba7f15506":32:"22e50ed0":0

AES-GCM NIST Validation (AES-192,128,1024,1024,32)
#1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"02bc0a8ab5468123009b2c69aaffd0a20a1fb082b55a7ecb":"
8bf32af1632a7903f00e801ee6e5c690147c021be6886cf2462b2172786ab296e0feb96648e4a602ae6dc45e2aa60e661
0356cde26b1dde3aa114c5449216a467fcde18332a6d482d24a1ee952379340d036a48b63efa092db4c30a95f402d57b
9c837183e900b47805f170cfe9e69baea2b939799e983f7470bb1297f937bbf":"bcfc15308e891f32506a50c4ed41bff6"
:"01bff5e606a536e951213b23672db9074fa8bbf947e815d32cbfe30adc1e736517f86139840a4aa0a671b4e9bbd6a59d
292db34cc87742c0dfd2d658ef157734c5fdebb3e5772d4990ad1b2675c23ddf1472e892dafe7bf140d614c50cf937923
491662299ab957606f4ca5eed2facdc5c657784bac871fab04d6cd3ccb18332":"b8dff03141832970c925e7ff0038394a
0df7f35add3046cc56f73e3eff59e18932aac697456107b6da7da3249049c3be5c098dd730cd4bf68cdf798c3a932b2c51
f18d29e4386cbf1b7998a81b603372337784307b0beb59235eba4d3e4810899f6d71a994ba9742aea1875878ccef1bf6
74ee655a0720bd37e44b33cafe5742":32:"bd0be868":0

AES-GCM NIST Validation (AES-192,128,1024,1024,32)
#2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"7c07d5ccaadb9e3ba5b5ddf380a7a2a175522b98e31e1d34":"
04d3e6bcd5ebf696fe84a702ffd5f76dcbe9679c909b36d41ce6362f229304aeb19896c6376cb3c25081f709af57d36f39
f421ecdb70bed9f829558bec6e78823275fc11f9a2d5f773d27136d903ff08e5926338dfdcbc182825794e5f739efc1f0ec
da8e53751edbe0d08963471fb5099f2ff31f76b479677bd6d186a409525":"e4db5c6403a03daa703516763052bce0":"b
747d97f263d0ff6119df1b5332640d2e4568813adc12ed76175fdfffafd087456748abb267195688d2db41caef3011179
79dfd2db9714b352398594005bebb449ea20415fcfb2671253f69bf6467ce7f5bce350a834c4586eb03e766c1930e7e6c
cf01283ea31b8c73d7967cde0f2a53cc46b1b50c48649044d6f753f1d54b5":"f5faf7bdd99c62ec87f93da2ca3ce31e694
df0a0fd04d61914f9a7a4235de20e0a406e297ba1099fff8c14e8fd37a9d6cbe2c5c572c988cb1ff87ffe7825e1947ea3da
73b8b3633721fb4e08deb3f8fcae2407d73bd4c07f32b4f9ad0b1364003b11f84037a28239e96c3996874ba8e4ec7270b
f0441d648f52f3730d30e3536":32:"e0820c4d":0

AES-GCM NIST Validation (AES-192,128,0,0,128)
#0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"dd01d48789ef7f07f80a7385e4d1b1734903bc6ec768c9f2":"
":"944ed7743be9ce370cba7b7c9b7dece2":"":"":128:"dfa0ab389c3a780f598af80200c84da8":0

AES-GCM NIST Validation (AES-192,128,0,0,128) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"0383849ed0db3e52743aa82fe8cd9173b457755be8bbd46c":
"":"c6b8518346ec52c001697b7bd38dc795":"":"":128:"48a1992549b627c8621e8fbaadacb16c":0

AES-GCM NIST Validation (AES-192,128,0,0,128) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"936388053ee0116b3f783ae34f000d5fe2c5d712842d46f9":"
":"c5426b20c014e472c7b85be2ed0f64c8":"":"":128:"4cf0f6a45f3544e3d391375c8fe176b1":0

AES-GCM NIST Validation (AES-192,128,0,0,120) #0
depends_on:MBEDTLS_AES_C

gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"40dfcb3151a8dab1cb79a6a1e6a24fb55024d0e256bd4b07":"":"b8495cc54653e7ad74206153ea64c3cb":"":"":120:"1d3786412e0ceb383de3898ef2cffe":0

AES-GCM NIST Validation
(AES-192,128,0,0,120) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"83ca41d8b33c6134a14d8b30b0c36d5b799574dd925f3b8b":"":"fb9aca5b4932035c65b571d170fdf524":"":"":120:"9787f7d68d2648963cb49fd7459121":0

AES-GCM NIST Validation (AES-192,128,0,0,120) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"886e646688d573c2dcc8ca229a11b394b3400408dd801503":"":"c0744685722cb87717c76fd09a721dac":"":"":120:"794fe4df0084c21ffeaf959e5b0382":0

AES-GCM NIST Validation (AES-192,128,0,0,112) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"0b845dc2c4e9e5a94bd3e8969300b16b45d3ad5eadb2e80a":"":"0900b3fa3cc9833d702655d285f904ed":"":"":112:"dc670518e150d326921bd5f43e80":0

AES-GCM NIST Validation (AES-192,128,0,0,112) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"ac9fac2e32ab44a0774949d53a62c1cda04b132a3b07a211":"":"8cf6a81bfa21633ad95ffc690c737511":"":"":112:"4cd7a6e4f3ec3d41d086e6abf14c":0

AES-GCM NIST Validation
(AES-192,128,0,0,112) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"9f9721ef784980d03140490f760313cc8a56424affb01672":"":"c104bd8482e3fe7359c85e0e94fd4070":"":"":112:"3f682fc71989804ba74bdad04a97":0

AES-GCM NIST Validation (AES-192,128,0,0,104) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"f7c935f56970678ab89f6d97315a33efae76148263e95f1e":"":"1a91965c5458f4a1fde309cd42a3f277":"":"":104:"ce266c6f0447623a3ef1f6f57c":0

AES-GCM NIST Validation (AES-192,128,0,0,104) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"30ecea6cac70a9de4f4f7f441d6b9b5608cca39d07c0ded5":"":"361e5cd21c670de39b5f0b2b89437f99":"":"":104:"48a9621522a98bc6c0acf03429":0

AES-GCM NIST Validation (AES-192,128,0,0,104) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"4fb80c4fd026c3f68ab8fcb8e28e144fdb3ba00d70295ebf":"":"ee552fb94a527d18d285d6c195ca7b2f":"":"":104:"5ec97630ce593e9d560136774c":0

AES-GCM NIST Validation (AES-192,128,0,0,96)
#0
depends_on:MBEDTLS_AES_C

gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"c0261023ee9f682789ce9ae970fb7601f07551259ef91945":"
":"bffe4af76db75bc4a3d42b57c73c51b6":"":"":96:"bf827b4526da77ab2e21908c":0

AES-GCM NIST Validation (AES-192,128,0,0,96) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"4fb4ab2071bff4ec239ac05c04800806df2c256a4845b13a":"
":"3ee0e2e72eea437e46a873bd659b1c4a":"":"":96:"572d3ec2650ad57eec84fe00":0

AES-GCM NIST Validation (AES-192,128,0,0,96) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"193d5ebeb466d3fe68754bba413c65112ae29c5ca5e450c4":"
":"04e9d31b3b1205cae37c435d5a5579df":"":"":96:"71004356f266688374437aef":0

AES-GCM NIST Validation (AES-192,128,0,0,64) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"9a455ea1d9a78425a41d43e293e88de40dd6ad9ab2a63ef0":"
":"c108c56a1b3261042adc89046ad1ecf8":"":"":64:"213d77ed0534cc20":0

AES-GCM NIST Validation (AES-192,128,0,0,64) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"d6fff8797db2f1884b7d71e3ef3e5983234a837dbd0c2cd6":"
":"6be4417d7c00fe9c731e0932a7037a71":"":"":64:"68b6c28786a017e7":0

AES-GCM
NIST Validation (AES-192,128,0,0,64) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"86e6c451ea0ecaec9e365bc4831e7a6c092b65ee9bcf1b86":"
":"6258168da407ce43cc18d6931497c1f3":"":"":64:"cbf20172e75a6316":0

AES-GCM NIST Validation (AES-192,128,0,0,32) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"9295cc6458d907da5e7c356a7de51eb8e8d3031f72a05fb7":"
":"c7eaad3389fc24a4ef96a711ffbfff9e":"":"":32:"12508e37":0

AES-GCM NIST Validation (AES-192,128,0,0,32) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"308b6ee958f81a7fbf3bc386e167459206df9c1cb999d904":"
":"2c61b991ce478d9aac818d7aa75ada36":"":"":32:"32ead170":0

AES-GCM NIST Validation (AES-192,128,0,0,32) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"873d033773218387690c2871448578d8440ef36553583928"
:"":"02072ec745c856c6e86873a0523d603a":"":"":32:"e6a5726b":0

AES-GCM
NIST Validation (AES-192,128,0,1024,128) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"cfd9c1375dfd19e64b5e4b75022fabaa049627d5238cba3a":"

":"0a745c6910b23c78b1b44c02f1ce11b2":"0cc6724b9f3675619fbc70117bfcfb5871e903b0f01382e404793c1dfaff5a5b4131a7fc3041014941dc2c53871bee3ff18c08e9abbb13a8ea220cb89cf65bea1581eb8ac43d148203532dad8854616210ed7f1f9467e6b22071ccc8bb7e3bd89a0ed02a7058401aa4f2b5d0ce050092b650591282e66ee789bbf032dc105503":"":128:"8ec41e9c76e96c031c18621b00c33a13":0

AES-GCM NIST Validation (AES-192,128,0,1024,128) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"6c9f16c5dff4bd8d1855995dcad1c4253759b6e2a833995b":"":"3f25e3210d6d9caa8725eb55c6813cef":"7c6a66d930c95ce1028310cfa3670b77ffeb5e9b627a667859665c1dee8e69930c287fb1f1a3706ed1a0d35eb6d1becb236352a226a5b686bc27e1e1dce4ac6d5974d88b9812b39ba289b2490821319b5fd677da23fab3adbae4fb3630e2571ac887ed951a49051b0cc551e7ebe924c0cbb1c516f71db60e24773430dc34f47b":"":128:"5e000478b55ecb080c1b685f24f255a9":0

AES-GCM
NIST Validation (AES-192,128,0,1024,128) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"a8e393e00714cd94de0347351b924ebd555003f3a297493f":"":"9c7eaf730fa8074acd372fdc53b726c0":"ce4cb46e67d85c5e68afe61ddecb1a36da4de42774d45250d0d52b328834385ce1ceba96f703daab81d7a981cd80c469855e14d834df41e4c0c98873f3dbb777fc0562f284c466b701a530f27fc4e6838cecbd162db34b8e8a23131d60d1f9dac6c14d32a2141173f59f057f38af51a89a9c783afd3410de3f2bbd07b90a4eb2":"":128:"66bb46adf7b981f7c7e39cfffc53390f":0

AES-GCM NIST Validation (AES-192,128,0,1024,120) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"bd356a8acd12b06de9f63825e93664cab1beae7f4112cc70":"":"72eaf459b8af0f787e91d117931e3cdd":"9295b227be3e1faf4e969be6c7f20d507431cf5da9e2a577c9b31538058472683bd52f0ad3f2fa9f68159c1df88e7dde40d6612f8abb0f11a0078419b34b558d9144ea6596a09e5d5548b275620e5a3096dceb2768d2f77a0b79e0b963387d3016ecc2f155d9182e3209d97c76329b830bb62df195cb2be11223565f496e751a":"":120:"2ff4aecc90e2de9a7d3d15eb314cc8":0

AES-GCM
NIST Validation (AES-192,128,0,1024,120) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"80ecc9587bc2cec1ba87ab431c7ed03926169c01eba19729":"":"5a65f279f453572e169db33807d9b52d":"29520d9020efa1ecf514e39a286f398c7225b945608d4b57ec873ae8bfbdd40e4cbd75b9b535c9f171cd7913ed4b21e09d6bb030eaa27ca58b08131817113c852b6cbdf550d94dddfde8595e689470cf92f9c20960b936ac0692171158e54041155482f29e4acae41565d87f5641d1aac96b8cb763b7f1267ccdbce234d067d4":"":120:"83dec0fb36463b86270656681455a0":0

AES-GCM NIST Validation (AES-192,128,0,1024,120) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"94345293fb7733fea9c8b94be2f4fc26f8c3655f583e2b0e":"":"8bad4f3f289b9f4063ba39622ba2b7ee":"7e2b6520d7a554e612d01f462606c0e6d0181bafece1daf54f4316d707483a5dcd4275a08caecc1c20f3e32872fe3e57fa62d598949f5e49ef0efd53e918617e0a140338c007025493f2e0f8dbe5fca4a57d1db6333551bbca79243a73ae8a68dafb3089998359159df916ee6ba4f928a6a173390f15f2ee6045d578dd757bb1":"":120:"da305181a12517420c6f0d71fd3ee1":0

AES-GCM

NIST Validation (AES-192,128,0,1024,112) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"a3915523031c3caa58ce02c2b1e6ee2eb42cdaf31332432c":"":"d5416986beb3131afd6b7967836d243b":"ba4e883147c8f07afc08735e6e439798bec60e00ed3f5982f66d6b82a9af7580934112a9858f83abbd71193190298f0683453d3f8388c475fbbc8f9b6a3d2c77046b73986a54cc4559c57cbb86330267e04bcf5fd583c6d2968a7971da64c99d98623676154b0ee413ba531ebf12fce5e06b4ee0617e43bdaeb408b54d1b4445":"":112:"f273fe664e5190a506da28ea8307":0

AES-GCM NIST Validation (AES-192,128,0,1024,112) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"799d3ff266644128f330ceb8c028297991b2a5593e4afa3b":"":"9d27061dd9d50817b3086f453f1f401a":"d3b5c420ac597daaac7503cd17f580e94ad779fae0d4199ada2c7da7c4a611228752375647a03241f29f810d3a6a74a140ef9651e4a6099259f7d41ec4e51a02917e8cc35edf7f60ffc473805f56f0ad51fcc767670157c050c3214d36f831a54bfeb7ab2039cb10f7919b89b0f623a572aaed313983b105fdff495d979b8a84":"":112:"e690c9afdecea2494b6cf5a576bd":0

AES-GCM
NIST Validation (AES-192,128,0,1024,112) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"7480905cee8be7f42b9490936041a19b060331712882da55":"":"27500a09506e0133c88f65e77721b547":"52832d4118fddf182b21513db25d54a19220335f8676ea35c0941d2a38a3aa536b8c9cbf093de83c6b24da3372baba2826289bb3cac415795b9bd3ea62bb9b48450978e79b936cd70cd551e580a6de3418a2be0f4c1f062954aed6adc94d805e59ff703d239fc2318b80cee45c57f916977b319a9ce884d7e02726fdb71c3287":"":112:"52a5721e98ba1a553d8e550f137c":0

AES-GCM NIST Validation (AES-192,128,0,1024,104) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"042db3f8af95ad68966bce9ca0297ed41b608683a37457f5":"":"32d3e97edd3f393da5abc3827cae1e67":"4d7c2ee6e024e95a6e684ded9898f5c7fae7da8658bdb40560dac6495e46a691e97c047e66046b55e8cf9b02d31d3caeebe3a9f8aeed756d6b0da1ac5d4ba2c5e7b54add22f681ab1d5a2ac1463e8447e08592e0c2f32605bd02f2f03c925a2159e5bdd880323f4ce18a826a00962ce418dbbd5c276e3ff30f1cbaa4795d1ce5":"":104:"e2afbb95a4944353ed21851f10":0

AES-GCM
NIST Validation (AES-192,128,0,1024,104) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"7f5ea90f99fc76594f0f06448321bd4bb5e494a5e351e41b":"":"002a5da3c543ca56dd7e5b013b094f70":"b8150b50e36de85158a96d2096678f31f179c8765ae6ba5723ca655e890528eae96d438f9d9365575dadea3cebb4d7df3a9d5323f93696c40781a6661dd4849531e672f5cee7cdfc529416c9c3faa889d0f66ee4049c949c3c8459680f490bbb0a25e50af54de57d9e3241e0dff72604af55827b9c4d61b7d1a89f551cea2956":"":104:"db9fd90a0be35a29f805989410":0

AES-GCM NIST Validation (AES-192,128,0,1024,104) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"da287d34379d56f542edb02ea673bac097150f87648a57b9":"":"6696034b1b362927b89ae1b7ab5297d7":"45818b7b69b05a121fe5c573c9903cb11477873b24a544ba919baec78d1565f4ad0766da58bfabfaa17ac3c628238a4d38b5c0b14b52e397bcac991408dd7b322ff614bd697ce2b5b94ca155a4442ddd9e502c4a5f81210c32dff33481f4211897db38f619b308f3708d554bdb6c7b8a4d2a80ccdfd5f70501c83502a312

ca8a":"":104:"8e65d86edc071446454a1bef34":0

AES-GCM
NIST Validation (AES-192,128,0,1024,96) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"1782ac334cbffc92769a170c3cd43915f735b4423ebb4dc3":"
":"736f2f24cd04e26d38e69c55b38cca7a":"5827d391efec2f8f102e5f053ac496e2910248a0eb72e8a0b3bf377c6349df
02ab0410a3d28bc27abc7cbe582a03000db57843565e4fb06c4078de75c3f1a21130d55befb7ecb919ad789a4de2816c
3a42d4e9b32e38d980c06045987d03739cbe7710d839c42f04f5088072c1a1044c3b89809b780e74e54ec135fbe4129e
e0":"":96:"c6dc3c4ae52f3948503d84a4":0

AES-GCM NIST Validation (AES-192,128,0,1024,96) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"20529c374f21c97b0a8f96f7bd5bdeb3fcd2b12db30b3ee4":"
":"e6e45b7c28f7fbcae658acb533614e48":"b41290031906709ec8048f450a940eff0422a6ebc7b44666c05f17aec9deb
c1bfecce62d896d5df4618517fb57ce7b04ef1579ebb2636da0eead063bc74ec184b0a69ca3eba675fc7107bb52a49f937
83608677565205ada7bf5a731441e44cede781120a026cc93cfe06a06fb3104a521c6987f1070823e5a880cbb3a8ecc88
":"":96:"e9ec5ad57892ce18babfde73":0

AES-GCM
NIST Validation (AES-192,128,0,1024,96) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"5634789b29e373760ecb9952f4b94ca76f40dda57ba363dd":
"":"7cd1d2d6beef44a6d6155181dfca3dc6":"0130a67935e2df082a95d0bc6dab17093fb08746a809cc82da7893c97c5
efc0065388bb85c9c2986a481cc4bbdeb6e0f62d6cd22b7785a1662c70ca92a796341e90a538fe6e072976d41f2f59787
d5a23c24d95a4ca73ce92a1048f0b1c79e454fb446d16587737f7cc335124b0a8fb32205e66b93bc135ad310b35eea0f6
70e":"":96:"4006685e2d317a1c74ef5024":0

AES-GCM NIST Validation (AES-192,128,0,1024,64) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"f0072110572321ad9804efb5bcbc2ae7b271b1cbb0f4897b":"
":"604ed8056666b17fd27b111afd419375":"97f68c00513b2247bc88a331a3ffa1208038736d6761b3b080884a8dd46
e0596f2c00c1a93bceeeee814210e57d7f1cbdb4e0c2ea6a0834baf716945af9aa98e2826ae0eb5717b241ede2b9e873f9
4c1db9eb5e1b25f75827c25849a2c7b92098b54845ed81f52871a2b0d12d317846cec34defaaafc3bd3cc53a6ab812bd2
50":"":64:"64881eaf78aeaa7d":0

AES-GCM
NIST Validation (AES-192,128,0,1024,64) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"e91e8c2d6928bbaf870e141ee34d3a56d00dacc8c7e50514":"
":"6f3d661a3e321844d1fc12d5ec2becf6":"fc8e5b45ad1647f9dbdbb6b437abecf0a8ac66065d0e250aa2ae75525455e
e13adce8c59d643b96de9002d780db64f1eb9d823c6b9a4238171db26bf5d05153d1e3c839b93495084363b845fed75
671ace0c009800454596674217b19832751252f051f3995776a89209c1636b4f4b28a364bccdedb78ad36876745c1a43
8406":"":64:"1f4f495adfed6c1e":0

AES-GCM NIST Validation (AES-192,128,0,1024,64) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"138ff9c8c556ffe7637f7602cae428d7e20dff882d44ddc3":"":

"38d7005fadee55b5a0434d924d971491":"3facceb047e486998c945839ee5eddd67054bbb28308365b2909dabaed29fd5b7b34644043fa443165e07b20214710cd652fecd816d9273c700d6828d216db8f3ceaa9eed0e251585f4ee5ba4beb3c0582b8128a3ecc01f4b29cab099ba2a8931e56120802fdf6004a6c02e6dd00257a83adc95b3acb270e8000fd2126b8eb83":"":64:"fa8aed1987868388":0

AES-GCM
NIST Validation (AES-192,128,0,1024,32) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"1187a34ccb75fc06dafeca0235186c64ba929adac6cf6e49":""
:"9dd515d3481f21efbe43198f623b34f7":"8a1b00ea5d1f4e451cea71b3d2fc9bb03b9790a8ae8ae262b3e97ebf34911f9d865c8810b9fe779fff701c72f3639654e60898d1f57eb93381749f0e2cecb4ee342f5f34473215d5c46818338ff688637217fdfa8b7ee552db01973fdb6084c3c20b530863eeb1ce798046890994f5625df2a56042d62742097cc10d512a543a"
:"":32:"83f45529":0

AES-GCM NIST Validation (AES-192,128,0,1024,32) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"4c1052610d05fb77543b6b517eb64b487ed902f9969a420f":
"":"90f4c93301371158271a8f46df1c86c9":"83d009a1238f8aa40e36cbddf08a5f3d96403a03f7d079359cd6d3d0c719bf79c908654882919dbc6c27db34007b6732cb344a0f4babd26b1209ce6b134a8d2318f9a38af034b265562097b63794d7efee306e97c6ac0a991b3764ecd936c87000fa58e6689e302f12c2851b1ffc950dad7a553c8c67e01a2270e1e5e9caf30a":"":32:"30b3fd85":0

AES-GCM
NIST Validation (AES-192,128,0,1024,32) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"3dc62e54957bdd1968be71b7d205fedaa291349d69f2854f":"
":"b8bce0f9263688ca41c4cefb26e79453":"22b6d92d8908bbdbcd0ff35299eddaf0cfb039befa2d2d83c896f373b92091d145f1771c58d60f94d3548d0cbbeabeb796d7632b5da3c66ef75cb41a35e7d1b032ccfbddbb9423e0ee054bd56b6288bdf1b616492c85393e4134ff9c066b23f3f626eac63a5fe191ce61810379c698de62922d3bdbe30697a3e3e78190756c3d":"":32:"67887aeb":0

AES-GCM NIST Validation (AES-192,128,1024,0,128) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"f170a6a76109035559296 8d67fb3514b8bfdb41cbf121341":"a050f858c87d56dfcba3ac1ccf5ba60628b3ab1b89845682a95b7f291c80f6eb1cbced4fa21e3584e21528746231e7311ec319a0fcecc329e1a7aaed0a8548e613e51db78c86c8d0cefa15e30b745b952809f87d8a4a7bbefc76a8eb824827d4334201bda7743dc497ef5fffa2812e67f2a04e5c10bf464179c6178db932ecd3":"e02ef73aee414041b137dd3cae8f2765":"
":"c08c9bccf298c8a352cd72e9174f57dc9bf64d65191a9e97b43ce70afacfe76feb5b2695d72ea4635fa94144de02a54333a77c7d4adcde17c166b303f1d664e6edb081a85433a7496f91ce640f113935cdd4e7ad14c95247506ddc6620913b5c67422f599ca00b95d62a9371e44c5af5295bf96743d0f1228c96e95af3b4d366":128:"d64d9ac91548dc1bad618509633e0c25":0

AES-GCM
NIST Validation (AES-192,128,1024,0,128) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"2ce5a40618b8bb2d9fc1d87a3333a9cd4945cfa838c8e0c6":"4ad4d103da3fb2ef8adcd1e0e823f4a857f1d6fa6273bb66574033c18ba2f760951ee0fdbe06c5cd3a0a30bd11142450f2d7e71af2fa7b9556b663fc30766508aa24e1fb2219f30ec23a6cd48b58944541d1f3e3fbf596e2ef263bddf789e7a666a6

8638081f0ec1a6cb3cb7feb0fddbe323b307675324ebceb25cba6d9002d4":"0c4b6c940d091efee98bf27fad79b04e":""
:"ad611dd6ebaeb5a634d4bfba9f965948ea79d16294b976b7c8bb57240c5d13e10a9fe7a5b5d39143000b4f24fc331cc
4988685c8d6401593a420c12e6cbd7cded06504d6a1034f70153f7b5019084a66ce818761841cab52d5bcb2a579a4acd
9df50caf582bc6da2b94d4b3b78922850993ccec560795417016e55cfab651473":128:"317596eefdc011081f1dda6dae
748a53":0

AES-GCM
NIST Validation (AES-192,128,1024,0,128) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"f71d789a63213bbe17aa14f2956e9da2496a1efd1a63f6a5":"f
5bf20dc6a11ce5142ff34d6c4771dbee4e74790c4ccd3cb5af408a5c7bd706bac550d7ed56805f550efc7648ab501fbbc6
3a1070402626c5788f076ae40e6bef2b9aab9a4bd8550fe38f7cdb0fcca2657ca26f1f729074326f45ae932182905d849b
1534d3effe20dbfc3fc26dc6453d6544d481e58891405dbf876d0f254e8":"17327996f18c7096fc5b8e375ed86f47":"":"
fed961a497502b2e49043ff29b9426a1e864a7fe0a88281a1572fbe62203f071710ea1d77873906369b195919a7bd5b44
cbabab6eee23c3692cb8b9e4db7ee595b8d4b063d209b11d64150c45545b7eda984144e1d336a3bd3f187834bbc6950
b3e7cd84895a3a5e27f8394a9aa9b657fba77181c9040b741c12fc40e849ba4b":128:"9dba8faf9d12905970ba0e29bc7
e9dc4":0

AES-GCM NIST Validation (AES-192,128,1024,0,120) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"83182ba753ac16554e873281599113b7620bdb042704bce8"
:"6915d46189fcb0f9ab9b838da2124ce06398d638fec9c1c53f07a43fa0ea09feb2bf868fd1dd521f301f9f38e2e767160
38f34cc0d18ab9bf27ac282dc349002427ca774e211027baacb9f6bfad6fd7885a665e508f654bb018f0323215153cd3a
5b3e7b83482c08cf07ee5ef91d64a671b3ef22801ff21cfae95d6843ccdc16":"805c6b736d62f69a4c2cd4aa3745a615":
"":"76dcefca6305ded697be4488513cc3fd3d9f08f06a7c1a9133b9b3fb0f44badf5c7544881b5babcb873cab912cc8a00
337fc36100e6a5ad998eac5d8568795b41166377c5114757044b9b73206d19fc34b6378a06d55b5d5e9498c7693e818
dd962af9b9da2345f4ebf152f33fe85f3398a65ad7dec823a1b1155c38cf67df84":120:"746c9972aa8481253d0d54db77
398a":0

AES-GCM
NIST Validation (AES-192,128,1024,0,120) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"b176e7a68da4c74aeb91760448c0257b1e17101299e1405c":
"691c436811f82e747468571f80fa8502ef5f25936fca58a8fb6b619a7a95f4938da558a3b26a2f09c8fc1f5bd347c7724d
9fa377d0a52094bfaac88f3fa9b3dacc2f56d880e825809533da5980a63e01d6199fbea07f3d070e29c5d50e1013224f0e
a86e7c008e3a2e63df394ef6ad93ea97d73fd4429feee495b144ef3a0d6c":"42e2e70b0096ebd489bfcf4d6ac0f2a4":"":"
81f9c34c5b0668fd58ec8822c6ba75bd7eb0d1741260fad6ad5e637903aa29d5f5facaccb4b885f62e10b7371f9b6b43e3
aeb69bc5093bcccd49f3ee744e49f87cd2a2c36c808c47e4687194cbfd4faec4da66b99e3d4ced9cb8ac6ffb94d7fef3ae2
b92b9f613f2bda3ca6c8efa9c6df8bec998e455f6eb48519e8f8ce4e526":120:"26d0921dbb7987ef4eb428c04a583d":0

AES-GCM
NIST Validation (AES-192,128,1024,0,120) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"8bab5bf1cd8f259129ce358cc56ace2bbbbaefa79727f66e":"5
7385955b9909a0856bf54ad25d00779cd7d3dea78e1ae8965c4b7a568934d15ba1a7b2ab899f69fb1b864bd4d529319b
51bf85a9b63de9cd51997ee4b2f015307cc42be9257e1b0a84e1c9e55a370476bff0a5325b21850f5b686a3bd4f1599f3
6d0772c406047b8ef29245c42ade862cb9d25b1e108db4f33a42dccf45c985":"ca5beea7dac2d9d24d548463977d5956
":"":"67deff1accc4f279ec2eb4c2a515c17886371bc4847bdaff4aa70e170775b64855a6fb0d347baf39bb53d7239b7a6

3ce451effc69e8d8c3e544b77c75170a68cbc45dc96ad238aabeb5ebec159f38089b08dfbbe94e1d3934a95bd70f0b799f
d84a8f563d629a5bfbb4eb3d4886b04e7dba5137d9255268dac36cbb5b5c8d35a":120:"f212eaad0e2616a02c1ec475c
039e0":0

AES-GCM
NIST Validation (AES-192,128,1024,0,112) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"bd0e0d0c7907bdb4b4e60510f73d8ab2a30700349206ce22":
"e6835a650047033a4940f72029857fae6fff2773f2aa0e4f7cb0a4abe86b6e8cb0c3e468637057f7eb20d1d30723e3c31
07d0f579e31a4c3e6fa8133e1b1b51fd21a8aa80ec657c4f674c032bc4a2d3e1389cb877883317c4451ab90692337bd8a
a6e9312388a0acddb508fa477cc30eb33a886e8fbced97492c9d3733cf3fc2":"1f183eea676c7ed2ead9a31928f4df5c":"
":"9f1a3017d16024dbfea4ba9df5154a6a2c794f00da070043c17f0204f06f637c8fffc760424187dce4fef044faccadefa1
b1bd818522915e389d307caa481af0f1f767c38216fa048f621d46880afca5c8fc582853dec95d19d19cc943e9a186159
7c99041c59e8bf8e7245f9e30b1f6607843a978d0ae7a4e0f716dabc9d9f6":112:"4ceea20bf9616eb73cac15fe7e2f":0

AES-GCM
NIST Validation (AES-192,128,1024,0,112) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"d59c476dcef60a45be253d5cfbb24742de9e3879bdfe6949":"
144696d85126c682f8446fcc2724fabe4b8840d46f3de6ae2ceacb2f06a1a80fed430e3a0242f4f7c308611c802c8b8e9c
992b78a5cf401fe7a4671bf081f97520919f02b66e8bffd4fe3f4a69cf3d16667e7724890cc4b66c6ae487d2d987bfacec4
24fdc9865af4474b04cce03fffc828b2df66d99087e63f35eca52abe864":"9bca808f02295477f2aa7f6ac1a7bfe5":"":"9
d23989edd8dd9911a3f5a80de051ec7812c6ce018e683751380ff990a079f3502ec0fabfcdacf6c1fb2503094124c39ec5
31b5d29ee8e4e46c324fc10dbe0f31e9aa56522bcc7085ccf768425227cbab6db4127671a4cab7bc65dc1d3d9d814694
93329e29a9a1cb7e5e088e84eb243493cdf1a49b16fc8d4ea2f142aa9ad23":112:"d8b20d72d95a44dfb899bc6aea25":0

AES-GCM NIST Validation (AES-192,128,1024,0,112) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"2f1594e840375405a682dbc1836344be8c6b3f3199ee7fd6":"
9bc6b715c65347a383f77000b3efb33b16019d01605159e09c116ded52d20721bcdde3796b6f4dc33cb29ce1c48438e9
5d4db6102465440cecaa50ca33ebce470d8986663652e069079f9d92ff167b3f7ae568218fc62ff5a7be50b3b987dab4fc
7979e5967bb0574de4bc51e774ba05f9780a49ac7b3ea46fdf35804e740812":"7f1f4a80210bcc243877fccd3e7cd42e":
"":"773d6901ea64d6840ded9a05a7351c0c74737ad27e7c3dbd38dedcdede94722ae67e88851ee471aefc1f80b29a731
2fa2a6f178ef2c9dde729717977e85783e2e49a1fa2e847d830fac181e95fe30077b338b9ac5d2cfa22ff9348a07710543
22bc717343b9a686dafda02d6354cf9b53c932da1712b9bb352b2380de3208530":112:"fc3e0ca7de8fb79eb6851b7bc
a16":0

AES-GCM
NIST Validation (AES-192,128,1024,0,104) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"88a6d441c1b7472aecf92c294f56f3c1da1702d174eff431":"e
ecc12fbd00c636a7ff897c244593239d2dbca9d1f370660c9bf9759cc41dc6e95075516f8d7fc06fa91ff6870177772517
1c2dc0767a1953fac13008d77065cce8ee329283d3f64adb8a298aa100c42e75d62e47fbf5134a21b826fcc89ebb18707
c0f4d54f6e93220484706a23a737341c601b56f6a28cc8659da56b6b51b1":"058a37eaee052daf7d1cd0e618f69a6c":""
:"0f5e889deff370810ed2911f349481dfb34e8a9623abd657a9a2dc14df43dc8917451ddeee5f967af832296b148d6a5d
267be4443e54cef2e21c06da74f9a614cf29ead3ca4f267068716a9fd208aefa6a9f4a8a40deee8c9fa7da76a70fcb4e6db
8abc566ccdf97688aaad1a889ac505792b5ede95c57422dfec785c5e471b0":104:"5fa75148886e255a4833850d7f":0

AES-GCM
NIST Validation (AES-192,128,1024,0,104) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"abb4c4f8d3c44f07d5a57acba6ccf7852030daa84d09e13a":"
24d82903e5074beb9a769f24a99b18c7b53c160a3c3ae4065335bec1c4170aa4c656bd7c87a8a13c0ffc6653c045445bf
8a135d25a13b2d44a32c219adc6ea2695fb9e8c65f3c454dc0e2772f4a4ce51ff62ad34064b31b0f664f635de0c46530c9
66b54e8a081042309afb8cf1f337625fa27c0cc9e628c4ae402cbf57b813a":"c9489a51152eec2f8f1699f733dc98f5":"":
"3e5528ab16aed5be8d016fe07f2ff7ac4d393439c4fe0d55437a68967d685815e359fdb8f77d68241940ce7b1947c5a9
8f515216254ac29977cc2a591fc8e580241442d08facbdbee9a9ff7cfbde7004346772b4607dafb91c8f66f712abee557d
3da675bb3130e978a1e692fa75236676b9205341ead5277cc306f05e4eaea0":104:"fecca951ba45f5a7829be8421e":0

AES-GCM
NIST Validation (AES-192,128,1024,0,104) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"cbce5e6d0fdcd3ab08ccd86115149b5569584dfadf40256d":"
3974339a1b90b19fd3857d812a0e59dcf43f9b0f360839940b99834ddedead79785396ab8fd0fc0e523c06f0555371fd5
bc857a95c3ead26536e6deb1faabdc776ac7cfec4b60d9c24b0856ecf381efd98f941d5b2a38108922d9cf1113d1e48435
4b55f9c0f09d95a77fd30ec9cc04d19199931e187c56fd231f96fce5e1eb4":"ae3a25be73876b6e9dc88573d617653a":"
":"4f57be0de00ca2c7c52c54b931c235fecb4ee1e5a30e29bf68f57248bafad87e484cc68465d9f64bbf502cefd2c84e55
96c3c8e58a9fb51a8c8b132579a94bc32e92f7c7247dc5f69fda98727c423de5430f01b37d77e3ae6bcd06eaf5625e5c7c
9c228b9dca5aad8f571369fe0964731bf1f143f2f709c7ed51641ecfc88ebc":104:"33375e21fd8df9f0196198b4b1":0

AES-GCM NIST Validation (AES-192,128,1024,0,96) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"96779eaa8699469e2a3bfae8a03fd4bff7abc62d427ff985":"a
343fd32fc513e0e9772acbf99feafe9de4b54e404807999b02e921e0914b2d64d0d402ef06f31e1db852899fb6db231ad
4465af015b0c16407fa3666ef5c2a6d52d5b4f60b0f7fbcb13574b2aa5183393f3a91b455a85b3ed99d619bc9c5c2dbcc
4f0a61a7b03e5ab98a99cee086be408ce394203f02d6d23a1e75df44a4a20":"cd7dca2969872581d51b24af40f22c6f":"
":"74422abbde6e4ab674025735874d95d9fe3015620a8f748dbed63ef0e2271063b6c0d65e00d41bcf4ea86ac8b922b4
d475f904c0724f0adebc2eef4a3abd0f9efd75408cc054cbd400436e0545e09e6b0bc83a9c7d1c1717589d180c7b1d4fe
4ca18bde4d9b6bc98481b7971c7eb81c391ac4dd79cdefeabb5bbc210d914d30c":96:"b0e425435fd2c8a911808ba5":0

AES-GCM
NIST Validation (AES-192,128,1024,0,96) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"39bfb4cf533d71c02932e1cd7b800dca9ce9bca843886962":"
de76f63ecf9c8d4643599f4dc3f9ed837924915ce4216759013cdb46daa0a508e06bcdb77437b0a58c40a0bd30a05ca41
433218c6869f1ecd26318aff27999a2ebbb651de8e03061b8ffe3e14060720eb35a8e4dfd8c870aa4562291e3758cc1ea
6c4b0fafcf210e10b31f8521bb0f6b29e8450b0cd6f8c8196ca2f7acb807a3":"d2b937bb5d2ea7d54d2b96826433f297":
"":"0b0b4c92f06b17103ed581fb32d46e874fea2a2171d32aac331daa4d6c863f844fbbad72e455cd5a3ef941d8cf667fe
d5855da6df0ccd0c61d99b2e40a0d697368138be510a2bf2e08a7648850d2410e4a179a6d0193e49a135524092ab1f84
2ed4057611daaeb93e7aa46e5618b354a1091a9e77fb92a8c3c0e8e017f72deb3":96:"a188107e506c91484e632229":0

AES-GCM
NIST Validation (AES-192,128,1024,0,96) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"41b7d80ae487ac35aa498e5939a0f27baeedf48a494c8e91":"
c26d4b918a0c967141fb5712a28698d16640d200b2934187b81ec58486b706ea1caaeb654e5fbbc0d078215aceed7d66

939e0fb54d6131d8948cf58ec9571646ca75a051c2b5c98fe16f7733d42e5897b0263272015042f3134143ea3b08bc65
292d8d31f30f2ed9830ccbfca2d33d290c28f4dad07c7137a4ca05f432a457c2":"626e1d936b38cf9c4c3a44ee669936e
d":"":"8998e799985890d0f7e8b0fc12a8a9c63171e456ef5cb211f836a2dc7c9e3f4d1cd6280f9b0c469b703c55876b57
cd1d8cef70dc745e3af8438d878cb2fe9fb1c5b2d9a2d90edf3bc5702ef3630d316574c07b5629f0db1510460af8e537dc
f28d9c5b5cec6996eaa3dcde3354e39f60d5d896d8bb92718a758adb5cb9cc17d5":96:"69901cbafe637de5963e7331":
0

AES-GCM
NIST Validation (AES-192,128,1024,0,64) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"2ecce8fb50a28a085af744b44bc0ea59d6bc2c8ff1f2ff8e":"54
300bfd55b227b4758cf64d8a3f56cb49b436adb4b927afa8c4b70d2584a6cba425af4fbc3840dd6f2e313f793cbc7aca82
19f171c809cf1eb9b4ae8a9d0cf1a7aa203d38d67cf7719ce2248d751e8605548118e5bb9ce364349944a2205e1b77137
270b83555d5d804edba2f74400f26d2d0d28eb29d7beb91e80ad66b60be":"b7e43d859697efe6681e8d0c66096d50":"
":"45dac078c05e6a2c480543d406c23f3dda63f2b616007d08fbfb075a90eefab8dfbc26d334266f5d72fbc52800cf457f
2bbc8062a895f75e86df7b8d87112386c9bad85573431ccfcef6a5e96d717fc37b08673bf4a5eecedf1a8215a8538e1ddb
11d31a24cb1497c7b5ba380576acb9d641d71412a675f29d7abd750d84dfd1":64:"2dfe162c577dc410":0

AES-GCM NIST Validation (AES-192,128,1024,0,64) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"6773e627f6c49a1687a3a75d2ee6754ebfc2628bdfceba28":"
eb0a64ad510968c68a816550d9fe2eccab3bd8409ab5a685a8638f81b4b50a9a96318bff4e86f7f6e9076960be8eef60e7
2cee4ea81f3ba269d8ab4c9581a54638421520a6411a83e9dc83b6981a9dcdd9e4a367d57f156d131cf385c01a736b32
7218e6b6468d317ff78a01f1588c359a3a9b188bbe5d3ffad6b57483a976d0":"ad85becb03a05caa4533b88940ca141a"
:"":"959658fdff5fd802fca5c5a79d59536ba8ef1359ac7bfff81264c7827bd31b8f02ecb54f309b442a54a5a57c588ace4
b49463f030b325880e7e334b43ab6a2fce469907055e548caffa2fe4679edbe291377c16c7096a48aef5659ad37702aed
774188cb4426c3b727878755d683ed8c163a98a05f069a0a3c22085600759170":64:"4c0f4621b04b5667":0

AES-GCM
NIST Validation (AES-192,128,1024,0,64) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"1c086f7404c14160f33d6efde231eda610f92fa55ac147b4":"f
c8e5cd81755e489de7e3ddd2b587149ee013bffa2ce198c514641b0e1659261edd60bdbfd873e30e399869748bfe56ba
543ceb9bf5fd0e7ba2b4dc175c52f28a8a02b4816f2056648e90faf654368c64f54fd50b41ea7ca199d766728980e2ebd1
1246c28cfc9a0a1e11cf0df7765819af23c70f920c3efb5e2663949aaa301":"71f154f1dc19bae34b58f3d160bb432a":""
:"6d60da2fd060d2aec35faf989d8df33f2413ba14842b0406e38a6a847e191eac9f4570cea647c3988faaa5505ea20f991
32df2a8799cf0543e204962da1fd4f60523d7149e0dee77c16590d7e114ac5d8f88fa371dcdd254eccaa8316ee922ba23a
0a07b289739413ddffc2c709c391afee9289252ddf3ddb62a4532a5515e35":64:"f47bae6488f038fe":0

AES-GCM
NIST Validation (AES-192,128,1024,0,32) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"bae1b3eef91ba79032117c60fb847d46f18175565d0ed10c":"
9b71eeccdc91cb5f7a567a9189774f4c30d96477b88ac553df66b78a56e5c9e0986a17d80c811116d31985acfbf9d7a9b
ed291aa2fb6329457a836b3f8f11c16416f0a3b86dd9c717c8a050c6ceb5c27d8e2ee0dbe63f3e1e4f0aff4809e1f6f6ed6
4d31d494b7399cfa0dd9446321bd4256a49d0793a10a670e3f086408428e":"cec8b66a657e4bdf693f48ac52e60770":"
":"015a318acb6198189ce908ab1af28578a37a48beeed772c6ed4dceb0a3bcb092df85f653234c56a25c075c8e028d4a8
d90d974fb0477834ae2de8d5df53d0d03a979450b6e7a66fdc9b11f879ea9072699837f2de7192156f8e5d9411fd83d97

d31fe63ece4e4326ff50a24fc75004a5ba2bd4845b29e0794696943dff1e5d6e":32:"9cf6f90a":0

AES-GCM
NIST Validation (AES-192,128,1024,0,32) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"7c1582240ad301f831902c66334546dd681c12308add0870":
"d4b716b49858a23aad478581cbb6dfd015ae550d76497229b5b1776e83f2ded8542675c63ca6a007a204b497ed2ef71
ca125d91f386be9b4213cd352a797a5d78a1373f00916bb993de14e1a0af67524acfcc9fd71daa32e5def9a3f2dab5b3bb
a4d2f9f2cfc5f52768b41157fe79d95229d0611944e8308ec76425a966b21ec":"b6f4f3959914df413b849d559dd43055
":"":"79964f8775c78009bca1b218c03056b659e5382e25e43759c8adfa78aec48d70b32ffd56b230fc1ce8c21636a80a8
c150e5dbb2bd3f51607d97ed097617963dc6e7653126fe40cb36a7f71051d77e4f3b768a85ee707c45d33cc67473f94c3
1da3e8b4c21859002331b5f7350e3e8f9806209255ceac7089176e9d6b70abd484":32:"79e5a00b":0

AES-GCM NIST Validation (AES-192,128,1024,0,32) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"fd55a356943824d20630b1539627ad1a9dcd8ee2cb4dbf49":
"b8d8d6dd0631f9183ca858033a31dd583d3ee3b9510fcc69d8cd412016bf854b9edcf65c2831e63d72f4cb61a99f6f4e
6dab0c2ce9c5a8cdbc179ae93aaca2c8a5b848a15309be9b34e5226aa9a5908f543fdda983fec02e4073edcc3985da522
2b53f8c84b9c54c78dd8b2712b59209463595c7552e28f2a45f51cb882c0354":"aa89a122c68e997d0326984fa5bef80
5":"":"107a9ed561e6c45c375d31dea321c7b4a4b7641024d2c9eef6a103a750ba15e1acacbcae121510b4f56f19d29e6f
b3e6fc06950b1daa521528f42284130a40e5a6c1b58b3b28003673511abcf59a4b9df1548a00f769d8681978b632f75e5
da2cf21b499a24fbdd4f7efe053d4a1b20b240856d3ae27948e35098aa617def5bd":32:"7f9c886a":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,128) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"4cddc8f525640fc0a0875c65b788ea75c673f84f4aacaed4":"5
5e3ccb855c1fd6d33e28d308485fd85abbd8ade1299936996851d44dde063ddc37962f9f67e95df02eaf3d87751624077
1c469be2abf2ef6c8dcbb79eb1976f825b109f752079957a7c981faa2fcea599cc52e262b84f4c2031821619f0be6fa3c3
8d660e9eb3e0d5de2da6b83de9866eb3efbc6a2dff27e52587c6f79e1c26":"1b883a89413f62dd6d507cd70c048855":"
eeaf21bc317660b0e2afb9cd5bd450ff0bfa6cfa7e49edad600f71b971347e93b9712a6e895540c665a1d8338f61b51da9
e0a4a9122409824287ba4bc06bdbba10290a40b31b5eae9dfeb6471f4a0a0c15c52a2c677c4d472630d4078ecf36dc60
08faa0235a688ebbe2662e46a49b1dd58cbee82f285f3cdebda1dc54673195":"18d11513661296035f6f42d264e0b4cc
7ec47f43b758c6dac95e5e3b3834362eb64447d923e107a60cd66ac359cf3a203f9070eab9fe61ae64a86606c9b50a97a
19e12f731de28719fe178c9713edbb4525b221f656a340c867405c41bed3bbcb9c6da5cc6a4d37acd7a55f251a50fa15e
a8f9b8955606eaa645c759ef2481e8":128:"dec3edc19fd39f29e67c9e78211c71ce":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,128) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"3b8c31830b1139a60425f6a34387f5ca2be6f5a5074adf13":"
95f4ea90729de0f0b890fdf697948053f656bddf57e3d461e7ee1770161904bb2cbc8c2f801481bb54145af760e91c8b3
0cb22faa87efcc6f01e3f798af0bd460475754726514d53f419af2f2c373c76f05bf57d3fc1b763f72ba0fd2682d9d1d76f
6ce8d55b56fc7ba883fad94f59d502244804bb87bd06f1217a4a6c5055b5":"ab5bf317ad1d6bec9cac8bc520a37b1d":"
5a47d7474be6c48fa4bdbb090f4b6da494f153a4c9c8561cae4fe883000b81769b46cd65f4ce34abc3e5c6880a21d12c1
86974b0c933a16ba33d511e79b5f994c38e383b93eea1259d38f9fb955480792206461dd29d6d3b8ff239ea6788c8e09
c15be99f094d2d5980c6c1a8efe0f97f58f7725a972111daeb87d862a90a7d0":"1d0211d7d7bc891e4fba1ba7d47ac5a4
f3b7ba49df69fcfde64bf8689b0eab379d2f5567fcff691836601b96c0a3b0ec14c03bc00e9682ef0043071507988cf145

3603d2aa3dc9fa490cdb0dd263b12733adb4d68a098e1ccd27c92fe1bb82fa4a94f8a1cc045a975ac368e3224ba8f5780
0455cc4047901bba6bf67d6e41f94":128:"23681228c722295c480397fc04c848a1":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,128) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"9c2386b948f59ce651888451021772287f14a92d807d88a8":
"44f00c8a7c84e8207ec15a7be0b79c88fa347e2c3d5e8d07234536d86513bc39bebfff02efb9ff27280eb37f7e8a60a426
538bc1e3830bca0e76faa33b30719fab51578d15df77893bce8740f50c491b8b9f1739a695c78406b5ee4d56f80d8d564
b586b0f22ffa86eca46a9d8134a9507c5b9ad82757ec51b18741abc61f23b":"7a1f7d0be4c7f8869432cb8b13527670":"
f76ea9d6e976616689709700a9638204e616f4c1c3a54a27fb0dc852990d81dfd6787aa5a83b9be5087d3f7dfcd522044
911fa4186511de1957b80338025c6c4aa72058aa3160047cf42166aa0089e2ec1ac8ea6d9f5f2c057f9f838a72319dbd7
bb4948da3bc87fc2036a0e7b5e8cee7f045463152ff80a1711ef1096e75463":"666c4d6d3f1bec49ba936eea90d864e8e
cbe0ccc7b23872a4ad7596afaec628a8165a70397289a10c67d62942e1c158f1489a9de44443ac4181e74ebf2562995c9
182b57bc960f4b5d3e33fb7cf7a0c32a59c716de23639de9bc430712524d74a087647e27ff1af87a2aa0cf0b58978ad8ed
616b566225d3aef2ef460be7393d":128:"53d926af7bbf7fba9798f895d182b09e":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,120) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"5852b4bbfa623e5e2f83b888f5eb6cbe06b57299e29a518c":"
8cc85e520b45a85c69cd80072642ef1500b1e0a409c435d685544a6b96d3224cc40e5fe8a21c4959b2891d4a53bbff03
db9939c655e6e92222c6b44c95204827bd800c74666db64907894bc4e3043fab318aa55a011ab9397592ced73f07a062
82c22d9a57dd7a37eadb02f59b879b030d0a5005226c461281ce3061bf26de56":"b96f4bda25857c28fdfa42bfe598f11
a":"0bfdc1b16eeae85d550a97a20211216a66b496c8c19030a263f896958e4d1decc310b955523e314647edcbe3f6997
0cda8e07f8b81f9074434fd86b8ec5b3fa8b155377ad28050b50523d3d185e5869bc9651d97c56ec6b8047c20d671f6d
c657f4cdf73fd7d3caf4b872f3fb6376eda11b80d99cf0e85c4957607a767642da6":"b148312074ecfc8f118e3800dbd17
226d55fc2c91bcbceeae2a7ca3b376f6d568dd7fcb5c0d09ce424868f1544097a0f966d354455e129096ec803a9435bbb
f8f16432d30991384b88d14bcad1191b82273157d646f7a98507dc0c95c33d22e0b721c046f1c13545f4ed2df631fd2b8
fc4940e10e3e66c0a4af089941a8ad94a":120:"e3f548e24a189dbbfd6ae6b9ee44c2":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,120) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"2bd897e969ccee405ba9becf24787a1e1be17a571442c6da":"
50b8ade5e6547c350c3f43a35a3cb641459c5ef902afc706ce2fb980b275fda62e8974d1577ef65ce9fd854d88caa10295
d1045ed7563e9391d60700b5d2a4a7ba5f3de7a7d1541780b95a08eb3f0996d96aac7ee838b67ee869447617684c0856
6647a4991e31829907ebe4b32cfa46c0433a64f864b8b9316cb0ec2578ccee":"fef6a08d92b5b9bdae4c368fcd0cf9e8":
"fb3144ec6d93704d625aa9e95be96351c6e25bccf1eaaaf9a1d405e679efe0f2da07510ab07533295a52cdc1f5a15ef5be
c9e72b199625730e1baf5c1482f362f485d74233fbf764d0b6363075cebd676920a0b315d680e899733d6da05d78765d
b159c4f942a31d115d53f1d89cd948bc99c03adad1eee8adcef7543f9dea39":"e65ed5b6d0f51f8876f483f3d8ab8fed78
ab6c2e1cf50693c8511e1cc9823e1030740ac33f05a5aa0d88205bb3071a087655f28eee7d0a07945d25e3dc00221a1da
de4170cab9084c47b82376d5d439bed99150811843b176543f7944b1dd9684fa9a52117c2335dda750d9de0d9b3ef71
8123b6534cb012080f6ef8eda8d4d6":120:"468546d4199b9d923a607a78fa4b40":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,120) #2
depends_on:MBEDTLS_AES_C

gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"12141d5834b8ca48b57e0892b6027c997669dac12fe60411":
"cf475b50672fd8cc4ba84d17ab1b733fee2073a584d5427155f144ddd945d4901d5a9d76e3d6ae55ab3f9514861c83bc
a7d53868f35bdc8606a167ac83591be30ddb954ee173ee172e8d7742a71c0fee04ccd16fb5d54a45820640405209e20f8
494f08d791a2a15f5cb848df689296a04e4b01e2c19bd8d9ca8b4525853549a":"b6dcb39939a31df176dcec87eb8db90
f":"daf4e0cd0b29343defb65562594b2b6fd3f005e6255500330f77a0550c1cfbade5f5973e836ce7046bc2b2ab8bb798
3830ce6ce148d0998116183d1aed320d28adef9ffab48e0f6d6451c98eb83fafc75fb054991d123965dbddcf74a2c01c74
6bbbc8276b77f6732cf364d8a4a5dbf5aedbbe16793e8c406ba609c90f0e7669":"4c2d979b9c2dc9cbbd6d4ed0409428
5a44df92e7ebcdee7feccf04c66c45137a7df12110b8af805f5cae9b4a225c3f8dcfd8f401e05c6ce937cbfc5620acdf3a49
17c5b857bff76f3d728cf6a82a5b356fb95d144125d53e568b313cef11c11585d310ca0f7f1234090b1b62536885e9e39
b969060ad3893e476e88941fe2cdd":120:"99cec94a68d3e2d21e30cb25d03cd2":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,112) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"14b9197b7980d95b71ce1a1de6577ce769d6af4cb45f7c8f":"
03b37942f12435f1c19dbcff496738207dc92edf1ab6935b564e693da1865da67fb51e8a838559ae1640da441f22ee797
87f1e909cf3c32187b41a48fbc595df1c097fb37881b329fd7b30dd1e05d6052fe81edf2e10786acc8aeeb4fac636aac94
32c3be3dafb55c76ec85cc13881735609773350b95eedbdb695b2de071a03":"cad0cfa7924e1e5cff90d749cfadf9f8":"
283c8a38c7fc9dce071d4ff9ed79002a6862f9718678b435534e43657a94178353b9ec7e5bb877db5e4f62a2ca6bd5575
62989363c6fdedbd7f0f3eeec5445c41a2a8bc98117a1443ad4d5dd63a07806622cca8ea6f9f6019bd511634db28651b9
16e2399bbd84b03f8ec696ed5846f30320adef22ae6d164aed09edcfa25027":"83940097301e9867623c107d4447b250
bf6db7d06f9e07b8d8bc6b72b079b725ea1f4b5f79bb80c518bc69a2bd73cf3aa7b88162773ac5b27a2dcccecce66e158
ec0875937910e0b6f396cc7d7cac5d53b0fddf3cd70b570a647245a5264927be1b2d9c46fbc6a630b21fead46c4f35af1d
163268e49a16083590893e6df4671":112:"3e3f677e68208208e5315b681b73":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,112) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"80e2eaa70362203b7561b135db581cf32e9cd816464f0b2e":
"62cc2db32584a8d90f348be32224bfdcefd1fd25c5cb05c7e74becb4b40ea09d6495f73adc1fd23d148c11849bd825efd
f15e144587f785770d2aef2788b748c338373a0ea43882141bc9f7c693a291c512cdcdea6d5defb2efa2324736df7fc4b4
34d7f4d423fb1b8853ec3fdf2c1c2881610a8d81da5de5e761f814ed38e35":"3d7e99ddea0baa45e2f9f2289d2182a3":"
71663fab717ec4d9da34d4851437f4504dbd71b65b0d04eccc513282c351925c23892958b4c9dc023c5a34944ef507e0
b40857d8b508ab7104d13c2fbfce2d086d466291aaa449ad36977837216a496ff375959afe4dd50dc2620a062c926b93
9ffdb144a656bc04bcca8d1d4fa0a9cb0a5d713721accef2d2c9688a77bb42bc":"1c56b492f50fc362c5bf70622f817e18
14ae0b69db7e3055fc9e690d2adb940f9a78cfd7e08044671913baec663d9f9af6dede42fe16d200e8421d22066009535
704b05b3775ac41359d7c2697e2f4bec40df69b242392eb30e2d8a664d84cf95ec21797f1ccddb72926cfdff22848d14e
373f5e6c3dd349196464c98dc38365":112:"e0c1b140cd7bc4ded916aab8780e":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,112) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"4b7aa649cb1488a658b4387451bf59852e845ec7d2273c69":
"245251595d10d719d8d00610d391735fad377b60d7430c7db488488c1ec25c12ee0dee3aac3d7dc19aa602924a1f27a
2cfa8f6354315db93b5e4d2b6e8402c4254921e683ca681dfb3c7f433a97f119e01f2acb20988dced8494e086395351f2
af356b11832472cbcb109c13ff92f10a4c8fe69bd264c8933cded19a980bdbd2":"07b50b1aacdadeb03e7488458db03aa
f":"2a7970ee97d612b63d2a0c29e5045ddfc6621c237bc270b3147fc0191de199b6923947e3bd3750de5155e1df29caf
96ac702f948c38619e218138945595156cc5f1dcfde0d1d6a5aec48ff37c9ff2b2209a904c59593779820ea68ad95898c7

ca0d0d81583c44feb0fec30665cc56620a8c9408e4275e60f5284ed7c0e58285d":"6bd53e4415765f387239c6664f837371b39f6d7ff22453211e91de5dd14272784fffb4f6b2c0bb8c6b7d1cafc55133aa0d54d410ae383008fdd876456550622322fbaa06df0a2d7ccf4cc170d1f98ec6a7ad524a3e5b07761f8ae53c9c8297faa5b5621c3854643e0085410daf5bf6c7e1f92bbbfc3691eeff1c5241d2307bbc2":112:"78d37215234f9a32571d0d8b1e51":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,104) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"512bbb490d062fe5ecc8e5ad95920a9e9b78bec6a7694dc2":"862f2724ad82a53e0574c0a2a0515bd86c5ed0b5ae92278a78ea1a90c03059d08a91d1a46678aef862b56d0320e970b7f941b784841b4d8a38d056f2bd352d48c0028086a36426bbc1436da9e021dcac705b6e03649b426cebd7a235f6d060ab6302d777fc9316db4a85e8c1387648a8f5ce2398a247413cb9374124449e498d":"2d14fb3e058f97b7c9e9edd1d97cac7e":"290078e63c81abfe99010b8344ff1a03dac095e2473d7a31888102e838768892e8216439dc3355aedd073892f4449d9d4d3ea6c25a9152c329d24cc73eaa0004832691740e60f17581201c8f7f4023d8e55faa3942ad725d21dade4c03c790b5370d4cad3923527c20ca925a2ce534a652ed7e032cb1c7906aebbdc24e6b39a4":"44e78cf3a2ce4a5e498315cb8d5e841f926408921f3665d533caebe0a7fa6c164b3d2c0b21ff3a608a7194e3194fda165ada8d5fc2e924316aa4ce201531b857877c5519f875eb49e5908d8d81b69472d03d08c785ee374c5fe91b16aee173761af7ff244571fd40aadabb360f38d301463e9da8cf8dc44d20848688ab3be47b":104:"6037cb18f8478630bc9d8090e2":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,104) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"d3964ee03ec5e500f2f8c05313b78615420183fe2950be32":"b9424e4a79a08a7937da1da15061c1eb9a873748691ec9c1fc76aaa164bd34873d07437d203c92c0e89c0c5befedfbb17f721f576473253617547206fb2b340945536cd7a049864d099419cf3f7a9154c0ac8d676b0e9ec02947caa4057560af347ddb46002703f3531f27b2197790ba135e3d3c0709c86f4781890deb50f3ba":"d3d4e5fdf6e36ac75b4d51c47ce5b8f9":"6146a97a2a1c709458bef5049088fdf339e4fe29cbdf519c93d525b71c9fb501c4b58bef49d43cc7699b18fc89cee1a4a45834f517214a77fb3b91d741977308e1585c474245802118d0e2c7003057c4a19752a143195ec2a57102cb2a127d2dbefe1168492e072e74c5f6ee102a0c371b1fe2ddfd8ecbc04c6f42befecd7d46":"a2ae334bac969072e754c0e37765ca6253744941a35587bb4feda54233a7a59f037e971d254c67948b16e4c35f306c0984f00465399405ce701ba554419a736cdff5a1b4ae5ab05e625c91651f74aa64c96ab628243d31021ad56f535eae33a885b45730268f900b6df0aff18a433e2823ddb0628a7026b86b3835160e5121b0":104:"817be7dcf7adef064161b6c42d":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,104) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"7a8049f521fe9a00f7bf566369e540a48ab59d83305e2829":"67243a336a10b82a0a8638b35dc147c14ac63b20977922a13de459ae2cfbdb262a79004c3a656dfbc073ec8878595e24998dc44b9435439af117c9635c479676f6edb8f522cf01571be5aa5b5bc7d1cc3264436566f8d3c684973d1e88d46282b53836a1ab5a698560e5bf7629ec12cb141867f684b369546a1d8bf48315b6c7":"e4d81f71e1de8cf4689bfe66a4647f15":"4cf6733482c218af832e99970d0717ac942ebace0fed4ce4dfa1f710b9e131a21cc03dd3ced25b78bccd1991a30bb53b463c1440b6543b19af91e31c18866c2acebb78c2a340b930518e61a63ff8d6a6e8e7960523de40a178614dad4ce5ab253e1090a097f8ec00dfeecb46aa0e8f772f01c4e706de7e824386a13944600542":"cfa8ba247ada9e6b3e5ab7dd0a7108574cc811c2986cad951168559ff697b77684880ec266f0b7d87a2ff559e368a85846becee312bb2991692d928a7c191cfdb7f1468f8b84be4bb592ea640743443bd4941a8b856c57be21eb22fcb3f6c0a80728ddc9dc5fab1c77dfceb91699009054c5a4eb0714a10b74cf0e09fa630299":104:"1dcee251cda10b2ea8f2bfe6a0":0

AES-GCM

NIST Validation (AES-192,128,1024,1024,96) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"657567a56e585c84e4033268f08f712aa280015b77cd657f":"
96d889651c4f3f5120bee233f6395fa0bbba1f6548b109be568ff96f11d24e34d67beb6c20268feba89240674b0b4552d
0a6455d43e8edf943da3d8d785a5221df8ddb3a98d2fc611ac7362aef71f8f004eb455a16d1dcac488ee83d4f11c4a00c2
9d9990c5a2a97b897d67e51faa40999b1e510ac62fa4859123cdb37d202ae":"94dc757b6bdbfe925b762923cd0a08ed":
"a2c54e8da7dca49c73550bd1f5e68449295f062d5dfe5aa4201bdf353a2a1ac9c3c61f2b5482184cef481fa378a1ea990
ce203c2c7d76993c62b415ece06b9b7caacec0c4147c0cbf292e528d97c1a176fcb1ca6147cfa4bcce92cbdfe617738a92
273282c7a65fcb997bceb867ce01ec74541582d3961dddf3a2af21cad3ce6":"55a5d07a77fc37090c4206f19483aa3cc0
3815194ded71c2b2806ad9563edfebfcf962806ba829373947e3e93f4f39794514ad7b6dbc626e29fbc35f90f573da33a
b6afb5c94383fd0fdd1ee074d650d192f6d08fbd1e24a6966a81a2ffd83fab644ee914952de77e9427262314ac47c11a44
bf7d2890f9b9980499bb6a1f692":96:"41c72043f6116ee6f7c11986":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,96) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"61159242d48c2ca0c30377ec2ad701135adb62d113c9f9ba":
"8ae40603f6cdae4b63ac7b18b4bcbb83c65867c2ae270102efb6f00aa8af5d0400dc95085910a50a16cbcf71f06c3f3ea
b71345d59c6054aaac02971111c7146add8c072158e0b374d481bb540036a136ccb91523f96f24ea237940ab011ad38f
2a3095c0785df91604be1fe7734cc4119b27aa784875d0a251c678900334a0b":"4fda7236bd6ebe0b316feeea31cb5ebc
":"ed28e9954634ec2c9e2df493062abf3ea3e199299053a15ce8d6fe051d1076287e4e7c0b2bab0a599b763a29d0aab6
80626f280c4f5ad94b7792d9af532681f6e4eb2672781f2342304daff902d03b396853eaf585af4d3bf5078d064e9eea6e
94e667722f15c004f4cf52253a5c65b75319b07ba539558d8a2b552390a21577":"dba251e35422f60f902f594bb58dce
37131e8ae06b5f40ad23c4a70a5e25fe24c76982c9bc11a7f4e3cc62d8c1326170432633eba1634972a9bcd093b08e1c6
3ece07c4be79cadc888b0408e40c09636e1cf1e5e9a6f2ea44eea5409a2ffe9c3ac9a18ad7aa9041f08eb109c01ed90732
a8afe0694319ef98a0269685b4d16b1":96:"b0feebfc8324fd1e9e40f7f0":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,96) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"5b4c37150f8bf0e14e0bfd37ac14e606dd273577007f24b4":"
48c6486b2691b86f5f107e8fe0122a821248206d2dd3ce898a2bb3772202ffe97292852bc61513529ad95faf6383b5f6c
5a7c16c4cbe33cb02e5e50f32db95ee2962aae1c9c0f5470b3baa216cc19be5ab86b53316beef14397effb8afba5b51590
74e26bf5dd3b700f4ea5abd43e93ca18494e1779b8c48fcd51f46664dd262":"664f553a14dcd4dcba42f06e10b186aa":"
4386e28ebd16d8276c6e84e1d7a3d9f1283e12cb177478ab46acb256b71df5a2da868134ed72ef43f73e8226df1f34e35
0b7f936bd43caff84a317b1e5b2e9a2b92ccab1e3e817f93222dd1e2cf870d45a8458e57948a649360c6e2439bbcc6823
83b50bcd3d8b000592c3ca599e598a03b9953af485f1ecc22501dcacb7110e":"05fdbb5ad403d64011e15d27cd6f5a22
47e018e479e58ad3fee1e0e8ddd9e114c0e82f2c947ff9af525ce752f4aea959463899542b85c9b413d065ea175103c3b3
c35f56eea52af2c54ec08a1d5b7cd5ee4f59de8be86512b770e42ab176b6b70ccbcd264d6d5cfdd2e52e618dc24251ac3
39ea38cdc446c778d2db3c7c3e93d":96:"77f32401db21adb775e7f1d0":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,64) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"531a380b109098eafd997bd25bfde4868d2a1ca781795e9a":"
466237db78d4c770a658b9693420a2e087c978fcc434c9ac82f3e2447b2fa08be32d2ce6da25846555ffe5764234b07b3
5dd1d1bcb710e8a49f918f2c873681f32765b092a836e9418faba61dc59a254c923159be16f585e526616fedd3acfe274
8ce19ee03868ea9836bee2c6acb1b821e231eb2d30d300387c93390d51e3a5":"ad079d0b958f09732aaa2158f6215573

":"09e002c2c48beaf1122411e8624522a9e90cc3f2a040c52ffcb91136519277c39fd6a79292b8835e0fbcaef22792181
06aaf75036590f8a46f6b6912053a3b391849f7e204f096288d6141d5f80c7f91dd2f2b6ebc1ced6af8216e0a594814b56
bd592df800299b29e26ed7461ba3f6f3cf151b9c10ad634a01d9c5e578aa372":"d1f49f94e6fbef7e21abad23e16c06fcd
fa75a8c342be67baea8e0e57dbcd2971276e993faa124ac81e6be18f68af303518efd926513cee9dbcc5ef6cf5e9c068a12
10e53fdd56776148d51597e359dbaa0570b4fe15476ccc9aa79f7c765755b6f694af4269b9e18fc62a0d47708bca67dcf
080e200718c22bac256f641e7a2":64:"01ec395c99a17db6":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,64) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"fbd7a92120ff973ec69b6a8189c6ea827ca20743a8781518":"
1583c1578a8c8d272a970f05d875f199e497c55f03f10f7bc934fee21c30379dad3c580b3f99304a5747b61fd43428506
439ede2c57f5229e13da9cb7cd6174cccbb397e98fb90455ccf3ea3b1304f432a070a2eb5205ed863326b3b86d4eb7f54
ee2ffcd50ed6ef01b3ee216c53f4f2659a88fb6343396b2ded0b389c6266c5":"57658c71b2c45f6ae2d1b6775a9731cf":
"45ca8a168ecca7a42847b779ef152766b902192db621d2770b56c7d592207afaf52d19a6059feb76e96b90628995bd6
517af3f114e97af8d602a493b77405e93095fee6761877dc292fab696a4303102dece60951cca20cacb171abdcfd0ef6da
6c90b44edba63b9b6087d876b3fff24dea909899ebd0d0371c424f51a9a84b8":"58a290cf0e774293d1b55f5ef8a305f6
8605c0c81668b8a1ba95fceeaa65229404e18fa54dd811a6af085c98b8854d0f956adc2aaad742cafa9ed53d7cb445451e
e7a4dc1e8399ec7e5b4d004ecd22496565bf444b2e3d82ddf6a6d5e6256c5095a699d7ff3f8cf2addec73e21013ee6f3df
c0a3abf316ea5ee1d6943bc394e1":64:"af737ec3512da2b4":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,64) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"54bfc8379e0a8180b931c5188c95ab3ed3461d6e9004d182":
"93327664eb576bbb64e4ff061874346b4e80a779cdeb1fbe630bf5e4307d4f2c5d5ecc94aa8bdea755c1af165fc8925bf
cdf128c1ee6571e9f8344b22dfc90ed893316031661a9438b305396f3a80452c9b11924163b7fc4422b00dc58ee0e674
710239975a2cf3253bf2601cd155e09547a5f3be1adda84a4b29631a8e13161":"9d15df8de4150f44d342f2031de3611
c":"63331936d2972abd44c1c9f62e42bfa932dff8cc75d9f555f5a7847d08558e76f5393e08909760edbef8d2922a7ca8
e1c0c505ca627c02af73253791bb35ff080b4db7dddf4c8b304999ff645227cd79f13ac87f9c963b93a79a0e946e5781cd
bf1b4b1967a75314f19c7219e3b69dc2c24ba09fbbdf7184278f82818bdd0958":"18ff87dccbc24c396190c7b37c4a77f
86e609db7fb2b326802714d0f196b00b84af887f1b3bd30ee0b0b192d0801ac4e59ac40e5c652b3da32aa024da3acf648
da0253674c391d260c0674853c7821861059772c9a7f2775a7ef77d1d31a6ec1c51c5f3089bb516f8cf52d5a15724281
086abd92a74d255b7cc84b5051be4e5b":64:"bf0f7f8084e79da5":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,32) #0
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"21b775ef8c40a5387d6c8eda4e90d0a00c795681a2887dfc":"
6346f84301d6d83e1c5bad44fa7e0821f35723713ee8d4a9e2bf15abf953425b09bd77b2360f4e62e82bf9e14e2b56be5
1d032aa8a96e894f19f3e84630f9eae831b329f7638b09de7210cd29778059ef1d0bc039c1e10405f3ae5e4ca33216adcf
c21869d9f825344d62b50bab03f7aa7b92fdb94951a68acd01f1dee75e428":"9763e6187d4b96b1801d1f6efe7e80a5":
"3bd523c16a0022b780ae8318a28f001502120bb26e2f65f4fe94019686f9d1df330e70cef1b2ba4b6ce1f7ef37750f47e
602843cbc5f13ff2ceadc5091eb3601604b70bd4acad3d61950b9dd2cbfd83a391223c8e09fddd4020c0f8a8a7057139f
d92f3bbe034f03cc48afdde064c8b13ea942ec0d621db959ec9d5fa95afe45":"f25408848bc27ab087b3ea053762837a5
34c3702dd8be01d79f075f61d76ac1d6557d392e1fab475cc7d13a5f6be6f0718bad71c3c85b5996bd3c0159e2649309
88e3ed506bcc94fabecfb58caaf56e2e4315bb50817cba765636d1faa91147b3880815eeb90d0934180e49132833abfa6
279247d9dd4048dff851e9a551ee1c":32:"d1fb9aed":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,32) #1
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"8a7d8197d9ceebd8e3f6b3bfb74877ccf649ac91d7057af5":"
37b01df357561f5aa43b5b4b0081148213f7b74babc80f4b3c6dd78ad17687f11443cd4a57f8d7a74ca3080e2a229f78d
8e6db276c1142d5f4ee764eaf09cfd70c596d7a2cad5360c2de20d5e17ec6e06a9b049bb10f8742a30a94270cc6d7709b
2f09f3cb8347e41117b7ddb99e4a939f3094c016330a8f170ccccb9d3651fb":"db5144951a9f1721397b7321713a723e"
:"ad72fa5a05adc40fb38245da019cbf50958ccfe26abf67dfdd49f4c4af6bda8bfc99d557913b2634c5c65d33ca909360a
df598b703db1dbcc29481b17ca42fce3315ea1454693b5843e751fafd78158fc040c1cbe607063ba9c0ac02ae4b88989e
3cc63adda8427032c70560349e1a8ec847906a9a7b0422a694a1f9eb2b3b72":"6985ec525cfe869e1709751eb6f1ff0aa
bcb39ae3aa708adc452ce1a8cad8ab4f1739f660b2841566f1f5c9e15e846de7f86ca1dc085188fcaa4a3f839ab2a5f0cfd
36e36965ae519fe14f98899ccb07a3ca15ec705e3160df6dbc37ab89c882012eefe51e4da8d6d6b84b3144ca87a90864ff
5390abfb92992e44c46807b3c8":32:"c51604f5":0

AES-GCM
NIST Validation (AES-192,128,1024,1024,32) #2
depends_on:MBEDTLS_AES_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_AES:"713358e746dd84ab27b8adb3b17ea59cd75fa6cb0c13d1a8":
"35b8b655efdf2d09f5ed0233c9eeb0b6f85e513834848cd594dba3c6e64f78e7af4a7a6d53bba7b43764334d6373360a
e3b73b1e765978dffa7dbd805fda7825b8e317e8d3f1314aa97f877be815439c5da845028d1686283735aefac79cdb9e0
2ec3590091cb507089b9174cd9a6111f446feead91f19b80fd222fc6299fd1c":"26ed909f5851961dd57fa950b437e17c
":"c9469ad408764cb7d417f800d3d84f03080cee9bbd53f652763accde5fba13a53a12d990094d587345da2cdc99357b
9afd63945ca07b760a2c2d4948dbadb1312670ccde87655a6a68edb5982d2fcf733bb4101d38cdb1a4942a5d410f4c45f
5ddf00889bc1fe5ec69b40ae8aaee60ee97bea096eeef0ea71736efdb0d8a5ec9":"cc3f9983e1d673ec2c86ae4c1e1b04e
30f9f395f67c36838e15ce825b05d37e9cd40041470224da345aa2da5dfb3e0c561dd05ba7984a1332541d58e8f9160e7
e8457e717bab203de3161a72b7aedfa53616b16ca77fd28d566fbf7431be559caa1a129b2f29b9c5bbf3eaba594d6650c
62907eb28e176f27c3be7a3aa24cef6":32:"5be7611b":0

AES-GCM
Bad IV (AES-192,128,0,0,32) #0
depends_on:MBEDTLS_AES_C
gcm_bad_parameters:MBEDTLS_CIPHER_ID_AES:MBEDTLS_GCM_ENCRYPT:"b10979797fb8f418a126120d
45106e1779b4538751a19bf6":"":"":"":32:MBEDTLS_ERR_GCM_BAD_INPUT

AES-GCM
Selftest
depends_on:MBEDTLS_AES_C
gcm_selftest:
This package of mbed TLS is specifically licensed under the GPL 2.0,
as can be found in: gpl-2.0.txt
AES-GCM NIST Validation (AES-256,128,0,0,128) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"2c186654406b2b92c9639a7189d4ab5ab0b9bb87c43005
027f3fa832fd3507b1":"":"3a0324d63a70400490c92e7604a3ba97":"":128:"4c61cd2e28a13d78a4e87ea7374dd01a":
"FAIL":0

AES-GCM NIST Validation (AES-256,128,0,0,128) #1

depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"747d01d82d7382b4263e7cbf25bd198a8a92faabf8d7367584c7e2fa506e9c5f":"":"7156358b203a44ef173706fdc81900f8":"":128:"9687fb231c4742a74d6bf78c62b8ac53":"":0

AES-GCM NIST Validation (AES-256,128,0,0,128) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"1cbe30216136b7eaf223e6a7b46c06625176d9a08182fa806a63d8b143aa768b":"":"4fe6ace582c4e26ce71ee7f756fb7a88":"":128:"d5bdf8ec2896acafb7022708d74646c7":"":0

AES-GCM NIST Validation (AES-256,128,0,0,120) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"f31194c83bb8da979a1eabb3337ceb3d38a663790da74380d8f94142ab8b8797":"":"404efd26b665c97ea75437892cf676b6":"":120:"e491075851eec28c723159cc1b2c76":"":0

AES-GCM
NIST Validation (AES-256,128,0,0,120) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"daeed52ae4bf5cbe1ad58ae4ccb3da81fb9c0b6f7619ca21979313ad9d3e83c1":"":"4037eadb11249884b6b38b5525ba2df4":"":120:"360c6ef41cbd9cd4a4e649712d2930":"":0

AES-GCM NIST Validation (AES-256,128,0,0,120) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"3ad81c34389406a965c60edb3214663ac4a6bd5cfd154ae8d9dc86dae93def64":"":"cebbce06a88852d3bb2978dbe2b5995a":"":120:"bd7ca9f6bd1099cde87c0f0d7cc887":"":0

AES-GCM NIST Validation (AES-256,128,0,0,112) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"4c152ba30aefa5b2a08b0b4d9bf3f16fc208bb0bc4c4eca9411dc262d9276bad":"":"008d040fbd7342464209f330cf56722c":"":112:"c87107585751e666bedae2b1b7e8":"FAIL":0

AES-GCM NIST Validation (AES-256,128,0,0,112) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"9aed4ae6b1d857fdcbe5aec6db38440613dcc49f24aa31fba1f300b2585723f1":"":"947c5f0432723f2d7b560eca90842df1":"":112:"7d331fedcea0fd1e9e6a84385467":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,0,0,112) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"cc80bc031676eff5f34dd076388a5130e985f9e06df4b4bf8490ff9ff20aae73":"":"51f639467083377795111d44f7d16592":"":112:"02d31f29e15f60ae3bee1ad7ea65":"":0

AES-GCM NIST Validation (AES-256,128,0,0,104) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"db7a40213b5b4b07e9900dc28f599403b0579cbce13fcd4

4dff090062f952686":"":"aea6f8690f865bca9f77a5ff843d2365":"":104:"7f2280776d6cd6802b3c85083c":"FAIL":0

AES-GCM NIST Validation (AES-256,128,0,0,104) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"299b874eaa8b7baf769f81f4988a41e2708ae928e69a5ba7b893e8e6b2db5c3b":"":"2aa04d85d2c0dc6f5294cb71c0d89ac1":"":104:"ea01723a22838ed65ceb80b1cf":"":0

AES-GCM NIST Validation
(AES-256,128,0,0,104) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"a6c7b4c8175db4cf23d0593ed8ea949043880fc02e2725f0ab90ae638f9dcfce":"":"ae07f8c7ac82c4f4c086e04a20db12bc":"":104:"1132e4fff06db51ff135ed9ced":"FAIL":0

AES-GCM NIST Validation (AES-256,128,0,0,96) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"b98e1bf76828b65a81005449971fdc8b11be546d31de6616cd73c5813050c326":"":"929b006eb30d69b49a7f52392d7d3f11":"":96:"33940d330f7c019a57b74f2d":"FAIL":0

AES-GCM NIST Validation (AES-256,128,0,0,96) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"09ccef64ae761a70fe16772cba462b058a69477c91595de26a5f1bd637c3816f":"":"e34b19381f05693f7606ce043626664d":"":96:"2adc2c45947bfa7faa5c464a":"FAIL":0

AES-GCM NIST Validation (AES-256,128,0,0,96) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"654cf46598e5ad3e243472a459bcd80f1e026a65429352dbd56e73fcc5895d1c":"":"a56f27709e670b85e5917d5c1d5b0cc2":"":96:"177b9a5e6d9731419dd33c5c":"":0

AES-GCM
NIST Validation (AES-256,128,0,0,64) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"84bca1b2768b9202bf194f2d5e5a0a5f51fd8bb725f2bab8a3fccbdb64a4ea70":"":"c45b2708c5bdf65ec6cc66b6dfb3623b":"":64:"fe82300adffd8c17":"FAIL":0

AES-GCM NIST Validation (AES-256,128,0,0,64) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"c8ae011795c9a60ad7660a31fe354fa6f7e9c2724d7a126436291680cd95c007":"":"1bd9ea6186450f9cd253ccfed2812b1c":"":64:"35214bbc510430e3":"":0

AES-GCM NIST Validation (AES-256,128,0,0,64) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"df2f0a8a3849f497d12bda44e12ce30a6957f3febcd5ec9bc134171326ca66d3":"":"728cb9608b67a489a382aa677b1f4f5b":"":64:"e2ef5d9cc5791c01":"":0

AES-GCM NIST Validation (AES-256,128,0,0,32) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"78e8a8ad1ecd17446cf9cd9c56facfd4e10faf5762da0fd0da177f6a9b9c3a71":"":"f169ce6f3ccc58f6434ae2b8ad1a63a1":"":32:"0fe57572":"":0

AES-GCM
NIST Validation (AES-256,128,0,0,32) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"02ca6d8a862e25db9d68e4404abc107e700135df4157cfb135ce98eaa33151c9":"":"7b722fdd43cff20832812f9baf2d6791":"":32:"72dea6cc":"FAIL":0

AES-GCM NIST Validation (AES-256,128,0,0,32) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"9a2b709dbcc3a4fb15b3ad541fb008c381b7e985b57df52f07ca7cd26ab1ecc4":"":"729baa4c0ef75ed8aae746376b39fe3c":"":32:"2a0d607c":"FAIL":0

AES-GCM NIST Validation (AES-256,128,0,1024,128) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"449d39f863e4909984b37f2e5c09ea4d4b3e9fac67bd57c299e4e1d1f084aaa3":"":"d8e9118f331bb5a359f0aa8882861b72":"4ddcae0bc24d622e12bdeaac73e8d1ab7957af051d27dfaafce53aeed4cdd3f989ea25989a2f41cfb3c38dbd841c5560b0b5ab1861b1fbcd236865d13da55b50219462e021f8a21848a64a85326031fcec8fe47a6ef4a435dd2b2fff637644ffcf3914ef2dfa5dd556421bfd297be150b31db039f0f2cc422b282e659e70cceb":128:"c595b9d99414891228c9fa5edb5fcce3":"":0

AES-GCM
NIST Validation (AES-256,128,0,1024,128) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"3e70e66813fc48f984dcda4d1c9c24f1d5d1b71ecfc8bb9581782e7cca5a5cc6":"":"d804f1051e72c9b7117002b862eb45ff":"0b1ab2b7a87cebac668c7a532fa8fa56a22cabf0c41fc1e6744ffe07c857c6865d623f508351f98f3f0c577d1eb94300a30a445472218c8ac626b0bee7d4c122d33f8130436a89add341e8ef7e00694afb4ad80d314d87ad3f921c7105eed05431b8151df7cff2c8e3790efd4acd3f60332dc7f34fdd90beef70f9093361d65b":128:"c09c2e3fdfefa222f7345ae4efb978fc":"FAIL":0

AES-GCM NIST Validation (AES-256,128,0,1024,128) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"8e534041090b45b80f287dc5fa20ebda017ad81b0530e680f62c6280fd8881af":"":"ead675b019ef5c6bbf4985f2a382d6c1":"b1db220052c4bebcef27eed6db0dc91be481179d71160c5a2ddb2fe497a05484840b04cce48980057d770fbbd0d5f3d5c633b55470617ad2cab5767188283310337825c4b0eafe13b5b11293dec230dad43b220885105767938c7ec4600fe063f98aa14bc6afb886fc874c10546749da295f571e696305bd9165486e29f43f52":128:"9aa0cdad5686ca515cd58aed94938ef4":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,0,1024,120) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"2de18874470c09db683cf45cd752bdfa8bf33e7967220b1a69f41f2a02da1d80":"":"af30eb2d0a0c2a50ea413f3285aa88d4":"22889b868d8ccc9f488406813caed199b23091ddd796c8632f564e7cf5a39dfb725266a931fec958659b6fc5b6b9343b8217edb0acb010afc9416601155262b57bd398d62f555953f0e15958e19ae004fbc9cb25e0269a9eaa38a4635a27bfa719fb249fa49337796bcf5f416bba87fbf3b19f0d8c11290c25ca50bbdc822f01":120:"646bbc9b14681af65b0d1c4c9f1d0d":"FAIL":0

AES-GCM NIST Validation (AES-256,128,0,1024,120) #1
depends_on:MBEDTLS_AES_C

gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"1a1bb9122e762ecd7ff861a1d65e52607d98e7ae5bd1c3a9
44e443710f3b0599":"":"32f99ea4cbf52c2701c2252e5e6c863d":"91b7a70c3a06c1f7f2ea584acb5dd76177ba07323c
94f2e8f7cbe93fc0bb7c389c3c88e16aa53174f0fc373bc778a6ccf91bf61b6e92c2969d3441eb17a0a835d30dcf882472
a6d3cb036533b04d79f05ebfaadf221ae1c14af3f02fa41867acfdfa35f81e8a9d11d42b9a63288c759063c0c3040c3e6ee
69cf7c75f9c33fea1":120:"a8e29e08623a3efdbbe8b111de30a4":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,0,1024,120) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"3bfad1e8f9850577f9ba3f290e9a5e91b494c2d995342203
62e171a7543177ac":"":"8410886b70c57d7ded8596443bd1b157":"ca801c83596795515ea931edba00e06e332bf8424
6b7036e10b317e2d09a51b2981fcb664ee3bf4180bb0b12ed1cda221abc6790b27c26914f5ef9cea9536e2453cd5b247c
b054e295c2687b725a97cbc484b8eb86c6ceee03bd07a54a9301a3ac0ddb23aecb825a238252e7575329058b40e75575
a7f16439edf5be163ce5f5":120:"e3645db0c600dba52044efcecfc331":"FAIL":0

AES-GCM NIST Validation (AES-256,128,0,1024,112) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"65debdf2f2191a6cd8de8ad4d5d4d0d8f731f67744e2545d
f6b2a7cba89c1ee0":"":"fdab2ee547dd8b6f5a4ea2dd19697b3e":"d2b0a0438ee0f145aec9a7ca452b788ecb473152b78
fb75f6ace721afc7b0ae1942049b790f3a5b6221a8760295659756d35347cc04029be03459f3e23a71209b4e0bbe13a25
3a888c83db23376d3a6d9a539f7c9fa4a12dc64297e7c93dfa0ab53ef76b6e1d95bf6f3d5e6ee8f08662fc03ec9d40eff0a
43f23ac313671bfd9":112:"c25fc157c3f2474885e2eea48aea":"":0

AES-GCM
NIST Validation (AES-256,128,0,1024,112) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"496ae810380460d40cd2fdae8c0739f16b87205cc7f57db0
a71a473eb361d570":"":"77233de96f5e1744337778212b411bd5":"85f5b54b4c4af5c808120bd28d98e44e96f412662
3e57684957e9fc4fd1a2d0583940b8fc8314a249325476e8d05247831b04709580ae714e8187cd38f9559419e14c9fc4f
8c454ec191b8ef2a3610988fe3339d0dc6b72f5978f9eff9d596dfabf27056e3a908c6497267461386e860f6b9d6552629
4bcb92908b5661b06b5a":112:"4ed91af6340e70b0c2b94ab6f82e":"FAIL":0

AES-GCM NIST Validation (AES-256,128,0,1024,112) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"aca188183b46139cc7cffc82a6aaaeb2fd73cecad14e75c66
3bd62daf1ec711d":"":"7bbf7fb55eb70cce94cc6a2b67de55ba":"015cfba90f069545fed60f31992ff3d3c3592eb91e7a5
3df5978ded64291954cb99a57de82d5398ce782b68d14ac04a8b425395bd076ead59eb445721bdb2f45e19fa08911780
0cbbac7b8313fb165ccb1122acb654e1242dc7fe6885ea1cbb7281b1270cfa1549cdfe9b47caf47b4ac3807e562e48c06
6566f5e606b5023b47":112:"3bcb5c2a4261d75bfa106fb25ee1":"":0

AES-GCM
NIST Validation (AES-256,128,0,1024,104) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"8cd6815f6ec15f03b7a53f159e877a5981e0ab7f6e6c261d
dde4b47cbb2f2366":"":"c431c07d9adf5f61204a017259cddd75":"4e1a835402bde4f5227e64b46a1f8d0f23a9434e18
9377fcdf1b9621ba1987eb86a7f3b97ed0babfd674e74c5604a03dd016d71000a72bbbd00a7f7fe56ad0fcb36a3e24dd0f
db63bd66d4db415f35012416ed599796ca3f678df7eb5a1b17f75abb348ddd3b366369a7b362c9488aedab836b61f9a1
58f0b129c8ca0a53a81e":104:"0e463806ff34e206f703dd96b3":"FAIL":0

AES-GCM NIST Validation (AES-256,128,0,1024,104) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"8f0a72abcda104aa7fae501f9a3b686d00d3f6fe984731db8a2865bfec587073":"":"ab8acd063775d1b1314f14e90fddd1be":"02c6d426e7f20b725d8cde0a6382e49b029b52126889013ef45251f27b2fadb95ca4a9a3b16ad06999eeca4a473e813045db4942e9b9ff2e5a5e429d9bac298372344d1b781d5facabf6d779643f31ada6124eb50aad599044b54279ec9b25714ac8a3b9ad2487cec7f4b1ee245d7be3d496d6af1d4cbee1c8201312541f3064":104:"3f0ccc134091e0c0425887b1b9":"":0

AES-GCM
NIST Validation (AES-256,128,0,1024,104) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"417135cad74280e6f8597dc791431c95cb8fa63bbf7197e3ab37c4b1d6d9438a":"":"0fe22d9ba1d0e32656e3a9f07a517a27":"a0b2712e81d329d5b076a4be2ad6823cee6dbd17d9a592d065bdebb92b1ff37a56bf2f5e5341f39c574246ccda19e5f35fede49c9ba958f3920cc5440fb404fab7846884ca0c2a3af5b51f4fe97a1395571319cc5b40f8aac986d77de280db82343983982638326ef003e0c013af19c34672975dc99ccc0853a1acf7c617d965":104:"888b836c9111073924a9b43069":"":0

AES-GCM NIST Validation (AES-256,128,0,1024,96) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"304824914e32ea0efd61be6972586093349bd2cc2cf0cff44be943682b2dbff5":"":"b6d927a71929029f6766be42746f7cb1":"7281c81c7514f4b17cb125c4649006ef8959a400a1e4d609d277e363e433725fa32346a10bcbd826b6afc8222158920d0a2db1e6fc915e81231c34c3941ecf3c6f94ffe2136190cae3dc39a4277acbc247f36291b5614a8433b1a0780434a6c50521b72ec25145bbd3b192647155d5dd9df9e66762d39592602ea99bf9bfff49":96:"b6044c4d7f59491f68b2c61e":"":0

AES-GCM
NIST Validation (AES-256,128,0,1024,96) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"8a10e9abe9389738e12a4bb6f553ae81e8bd320e0dfbc05fbae2128c1fde7a23":"":"6da44354e198e3beb54792718becbcc1":"199d754630135b669bf2ec581d3027a569412ab39a78dd9d482e87b778ec65c6473656260c27827e00e566f1e3728fd7bc1853a39d00e43752c6f62c6f9b542a302eea4fd314473674f6926a878ec1e4b475d889126ce6317115aea7660b86ab7f7595695787f6954903f72361c917523615a86d6ce724bd4a20c9257984c0c6":96:"5c5683e587baf2bd32de3df5":"":0

AES-GCM NIST Validation (AES-256,128,0,1024,96)
#2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"d164ffde5dd684becaf73e9667e3e6acb316682c41aea247899e104a54dd7a7f":"":"1d388e19e9d7a9750e2fc1187d4b075a":"f166a5b6f91261cda56f1a537f42ffb8aed10af5e0248f8910034b92dbc58d25953f1497f571d31fbf5ec30d92234b440161703851f0e43530418147ce6270fbcb5db33ab819ba8973051908704b6bea8aaca0718947e6aa82498a6e26a813981783ed9bf9d02eb1ea60927530c4700ff21f00179002b27903dd4103bbc5c645":96:"52e10495105799ead991547b":"":0

AES-GCM NIST Validation (AES-256,128,0,1024,64) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"2854188c28b15af4b8e528ab25c0950fc1384976f242716c91bddeec06f2fdea":"":"075af9c31f5252b8920092cbd999e7a0":"e9452f71093843a025bb5f655eb6a4e8316ab59464

84b11818f22b62f4df75d5891fa3397537093a261dc9a7648b7477ea1f5fc761716e302763364bcab7992595edd0fc1c7
f7ac719c879e6616e2007948eb8530065a6cccf73d0fe4a0598819b471b0856e6d90ea0fc0e5d36a30ee925b6b8e5dbf4
0e77f01efe782c0bb4f7":64:"6ff8fd87e5a31eb6":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,0,1024,64) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"2bfc445ac0365ae6c3c3815fd18bbd0c60ea224f6620d9b6
ac442a500221f104":"":"43c5f3367a9955aaee1a0c4d4a330059":"db0bae8ce7c66a8ba2fedec22f236212e9a7ad72b37
1de285c7dc6d2f6c22df0ce4920e0f03f91eb1653c4490050b9f18a2a047115796f0adc41707d1ffcbf148aed5c82013f5
57e6c28f49434fc4eb20112f43566f212c48cec9894ac40772fcd9b611ee9444df7b73e35b8a38428ccb064c9c50491d2
535e0b539f424db83e":64:"49aaa806cb2eeadd":"FAIL":0

AES-GCM NIST Validation (AES-256,128,0,1024,64) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"7b828f99aaf751bf22d993ed682e488595617a607ed74aaa
cbb6b60457453080":"":"d48dac1d8d77e245420feb2598812418":"f50f785f4e7c848a55a616ecf4b6b1e1ca85e16de7
100c7e4273d411bd95c1380ee157ba501ba9616980195f34e39f43e335f33253342feb8ed64443483c721b85241a0320
b3cac83104de2db47188c61a373fba592ea16feeefdee1f2bb43927396f58151418672ebb74afff5c029503a0d0be81430
e81ed443e08b74c03183":64:"a5b71ecf845b25d0":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,0,1024,32) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"7b6da11d69fca3e4c907628d3eb63d95c7e502fc901372fd
097e064e70831432":"":"6fe2148f250ea178d4c8ca8423ead87d":"a8097bb74ded776f578eb7588f5ef8915db9bfa726
2af700c8e76ee114e07557b6786dd5a60a66b2703e7c9de5d6b42aca92568aec5d1ecc298dbd0edb150b8cc13c9a7869
8f7674caa94da6cacd1f3ef4ca4238c59830ea725ab3a6284e28966c8c32d9bccfb0cfd6583a5ca309debe86549a6f317d
15c5f928cbc7f473310c":32:"e9cdbc52":"FAIL":0

AES-GCM NIST Validation (AES-256,128,0,1024,32) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"c5ae9328be49e761064080fc213e53e373fd86359a09d03
55e2d438d9b8e68f1":"":"a7e3f8660ff925d5c88c5aceffbd7026":"2ddddba7a56cc808aec4602f09ae9bd78887827bf0
315d8dbe16821606ef9d117746dd138bf1f23565d1ab8f4cee36d53fe3730632c5df9f12109b16edbeae285bb49dfdd15
5f5dc97b319a85362d53cc86817b7c1c31e5e87c9f37422f133d00dd0776bd92ab05ce6860573cd911645cfe3fbe515e8
5f744899a447fe443653":32:"e35dbac8":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,0,1024,32) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"e4f8ca13ba86c658cc7f42d4f029422209efbd101bc10a1df
81a42cfb3a0f79f":"":"1a362fa0e4054ba11e4b06d59c8bc9cf":"e7ad5c75aa13659f8ce4b1650c46382645ec67418199
b84ea445b8ceef619ef3fbde59ed3d313c459e36fcf87d26ef2b453409b32f1086934c3072c1ef0aac83762d28b1193b9a
fff2c083ce4300b768b0ae23ff9d3dcf65bc1693f1350da65180620aab205aceacfc683c8be53a332e2d0337a7518d2a52
04f9c8d7325a4799":32:"e7a37f15":"FAIL":0

AES-GCM NIST Validation (AES-256,128,1024,0,128) #0

depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"00050a21ca1e72cd0924be31b943c60854be6744577de3d
d9d1f4fada4a19ea6":"693ffd3d92294857a99c702a0799eeca28ab066dd90917b9ea5ef8f6547f1d90b106cbec8ef2c22
af9f8efa6c652f2f97c2baf33af14fe9def230d49524bd65909c3df1490f637f99e788dcc042b40e00bd524c91e2427ef99
1bf77e7b2f770cda6e90076c5dac4cac7ee3958b53ff8ce846c3a96281f53c2c52f5f3e523536f":"2fc1afc1395d8409919
248709f468496":"":128:"e39b6a7fd5ac67a2a1cc24d5eb9d9c74":"cfcd6b9ff7641829cbadeaa2e56f1f150a099eccf3e
378fa4da59794dcc4490aa4f9c5db0ab245bec36a7d4557a572008e42f03bc1baff3c946f23f54a4dc9828f106cf4264e4
ab40165839d1085e7795b1ae0950f0ee4a08e46ada501b6b51dee0e518129c9426e5bd44c66674a9f99cfe676f002cfd3
44c5bbd22d3d91e600":0

AES-GCM
NIST Validation (AES-256,128,1024,0,128) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"f10965a66255f0c3515af497ccbb257a09f22ec2d57c5eda
e322a3e6d2d188ef":"91598690edf2de8b27f9bc7461a84e80811cee544f0542923898328cf157590251f0342cb81d35
9b5dccc5391a12320d1444c26f24178977dd6705c2b365dc1ece0152c42e2f0ee3162cf886ef5529f4f16a77f3bdd2aecc
d405b59addf098521d0d38cc25f1991e11be7ecf24caedb48a2a286d2e560a38fa9001c5a228c4d1":"c571ce0e911de5d
883dc4a0787483235":"":128:"6d9d3a5dbc8dce385f092fff14bfffda":"2867996e389e09ec0da94d42e77b1e436b5006
5b09ca4adf1cd03240444ee699dbb7b3fc081a1869ca607d77d5ff9754fc3c997ff0a4ee17543a2ba77886b88a7128bcc5
1d3450df58ff3a26671b02c1d213df6adb6f7e853080eb46b504517cbaea162710a9bbc2da8b552eb6b0e0cb98e44fcab
0a157312be67974678d143e":0

AES-GCM
NIST Validation (AES-256,128,1024,0,128) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"4437ee7d16d8c3ca1aa01e20b66749efa901614d4bb4bee
786ad5a5f1bfde2e6":"ff80727a3485cdbc7fab4ee9fadfdc621c538e2055706629046078f1aa3fb687fc728d3a7ffa52ae
457b7b5649613eab7bafa464bb435314c49e5900750f7ad39ca9b75df6b2eaa755439e101f67b7ae4cd80dc4a9dea0027
048253f2d0a6014056ca69b8c85605b00cf75fa7634a0ddf464270a8c79ce1a1324c4a4c513b24b":"275393276745bc4
3bae4af1e5d43a31e":"":128:"a82ff1e87d26e4d6e417b60fb2d3ce23":"88f994d276ed20be3932d16f551c4b7e2ed804
11f2e72ce098fa0b70c22157a59edab30649fec447dd63f0c87dceca7238ef0d9561b58489ba7bd86f2892743099f40af6
3c432f78ac0ad0b5c2be47b9e3045e7237b096ee400f430af63a6f309de785caf190f3f4aabbe79f727a741590de542bd3
43df68d13db55a5f8bab41":0

AES-GCM NIST Validation (AES-256,128,1024,0,120) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"fe4ec037ce563dadee435cfcb2bf090f1f7ccc7d1b5b4fab2f
1b738348f8ed2f":"64eb8a4bda9804c09b04cfcd89094928c21480908b81ee19d6c29c2a3631b1a5bdc8e7f8ea56f7b8b
8e14a5208296026785cac3a6afa54be8af4d5faedcd12b6621bde0f8ec5a2635fe72a89468ca7704c73aa40cd2ba97aef0
8886b27a694d339b00e7d12a31308672f87c06a7388a1432f869eb4cc1da864140b1b33931925":"47f5264f7a5b65b6
71892a05fa556f63":"":120:"660462b4088f6628a630f2e4170b21":"4a310e035361f98b8c54fb4cef70b1a9c910552ec
e056ca8fdab54c52308ec0ad7fe9dd1dae92badab5010577de522088768fa6466fbccce22e14c51ca7986c4063d0f06bf5
78dab16a91856713198a7138395c49c78b6314b57ab72fd079028c8dc351952d90b04a7cd2b245df0c0522447cdb7d3
329fd9425fe5cb40a8e7c9":0

AES-GCM
NIST Validation (AES-256,128,1024,0,120) #1
depends_on:MBEDTLS_AES_C

gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"e6e1ada628ca76eb9832cc6b5efc5c9d2686bb587366a6de2d734233fa95279e":"a0ac738e0fb35246b84a6fbe319f827039515df25d0c0fc6de7c048253ae63d3c561e44a12672ffeae1cb925610b482aa422bbee0e1784fc69baac3a97d69f51e6d2a17957b44b318624ea7ec680a559f4d3f2761d09bee66efb3a312ae6b3ecb673e756b2a0f654671e82500e7ace91f2be2a74bc3bc1ec1a4b6877a53c27c8":"5a100b451e3a63a3e6d4b8a9e59c6bce":"":120:"88df9a1ea54e5bd2ef24da6880b79d":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,1024,0,120) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"cd5c1e90d78213155c51767c52c290b3d657db8414ee0a7604a2ec7b48105667":"8e987693da0fb77b6d1282eebd3a03e05d9955ff81929b1a2c721574862a067ddee392c7ece52ca1451f3e6e321d7208882d97b4149af6d78d65c054e1bfcdfa62bd2202de32dea8363f8d7f041891ce281840f3cd906ab46ca748e5b3b11890b4014bf0271c9427c874097782d1c13dbb40e78fc8276fc134f3c29923a43a01":"4e022d8d86efbd347e8cbab7e979771f":"":120:"e7df79af0aef011299c3b882e3a45b":"3b20473d9b5018d089e7f74d3fef22ec2805948a9e07689831973c704a6d8db4d090af88d696ab8c3aae9740a2bbd7f03e0b18b2b591e59c335c1043a2578a89b1a9f20fd0dd53f12e00e9bfdb27de8caac772bbfc4de9e4a255a5d1b04e59625a87b8279babe613def58d890d5502abf2f709aab625dcc20c58772832c7bbab":0

AES-GCM
NIST Validation (AES-256,128,1024,0,112) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"6e3dfc07003bb6a2d82bd5263b2832f47db4e73279266c7a9ea21f4f18eddf83":"a960da222af9d4da5797e6957d59b00f6d3893599c70e95c0984b56eb3329b191703c2532f3288b15ebf655b9b5ee4617484e5ac9c39bb06731d03ebe4fef9495d003b0ed694cf540b4dc759d32629e55512680badd81234bd71ffd55fcb5e6a85031c1dc31ee1ed198939582d8336c905717cc87101dcfcf9d833fac815c8ea":"7c0f49fb54f5e68c84e81add009284e6":"":112:"b2ec0f3da02a9eb3132fb4ebe3b8":"a40b6f70f0572fe0bc70d83368e7c154f7dbd501f52501630a2e523d18e216e07368521f6040d806299397722b99bcf7f85d36b8bed934b49aa1fa76d38783e6a2e392d6d0786d467f7bc894a739ecf94f0fe884a9c391154f8326bf31ea5242a18aa263d04da4b63b11de23b42d3e10a2d5460cb32700cdf50a0d89165ba22a":0

AES-GCM NIST Validation (AES-256,128,1024,0,112) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"4103b1ddff87a508a219c808a04ad4750668688f4c2ee75b92d28d70b98a2c94":"a00a196193ff07006b7df524824bd0971d63f447a3a7bb1b75c1e2d11789482c115cff677b54948d36dc4de34200bce97be0101d88cee39b177857dd5da3cb0d2f9d6e1150f72a3bd655e0bace1d25a657ba9a7f8dff082b4460432075afb20173da22b49beeb6a030d72ba07869ff4389fc1c28d87018d7c1a9829c21932197":"5cea906737518c2cb901016e30206276":"":112:"3a3a771dd5f31c977e154ef5c73a":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,1024,0,112) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"cd8c2f0c330d5db316dae7a16b57d681ca058864f7bd60f3d0de174442283f77":"e2a5ad295d35031535bf13c2993bd0b292e8a9465b9dab738e59ba03670248a1ecc92b38a55bae34729162271cc1572c35fcccb27417b48dfcbff852a7a8845cc829a4461061b558ac8b5930a5c6491ffba04a9d0dff220b3cd5e4fc2e0f3db3b2ddd90328f2cad819573a7856299620b02f5ee0267f3b56981afbf1b7d9e3e1":"387ee8c1e7f047e94d06d0322eec02fc":"":112:"62356850d12b54e39872357cfa03":"17b7f6bdfc1993c56dd9bd674cc276a55a46fdd9fd5fe435b9e4b7ebc7052a9dc76a99e4e43aba7d486603189c90d10a21ad3722c86bf5bc856a0f930ff5bca65be708b76bb8a29105da67f31eebcec81f28aaf526d2f8f0feac393a24959dcd612e2b93b4463f61957d2b3046bcdf855e346601e4c7

760c0ca618ee7bf55381":0

AES-GCM
NIST Validation (AES-256,128,1024,0,104) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"7e19e400872eed721d560202cd757d3eb99729496b6e3a6
d38dd8afe1066045a":"3fb9abc7aba654dfb174e8899c17db222ffbb387b7260fc6f015b54f1cd74284c516e21aae3b72
338e5e8dc643cfafca0678f5bda3a7539f1612dddb04366031b5a3eda55f3232c1b176cc9be7cc07e0ebca674a2722249
29c401a2530efc6d4eed0087b544b12d172a01bc8340d9c2a2ebcb5af8b07d96073a879fda140c196":"d2b277f78e98f
1fa16f977ce72ee22a7":"":104:"4c81c044101f458fdfac9ca3b9":"FAIL":0

AES-GCM NIST Validation (AES-256,128,1024,0,104) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"d0653934a16fd36c27d54488a1829302b931bed6e26ca26
047242b85b50bfb61":"c02347e1add9178d830d8baaad9aeee37e958bedf2cc846e2561fe8c83481d0a8a85911e7f1f6e
444b28f30bd96c13c390e80f616feb6844ee6fa486543a2e3f38c138f45b4405e3fb331b64648219aaf1d574be948ccfca
6afc18d12488db19c35b05601e47c0af5d49a93a5dd4420f38585c1eb033e173376fa390d3f948df":"94886a1845aebba
5ed6b86f580be47f9":"":104:"4be34ff42085ef4443c8b6042d":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,1024,0,104) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"d0f0ccb88c7cec9496f26a59ddc67dc59ebe49ae3dd89ef3
be008598727e214c":"7845e155f4f28021291e7c814a1ace8f42b239990831aa82758fc1e376cace0b6f668f7f2f224ded
e1ef5b1df7ae74b2c01483701044acbbb72a9216eec6b7ef0190f114b3c73c6985c4653f11601c774d10b7f9df1f1e1f3ff
4fafa20d6525edb37d9e5acfafe6d3468ee068d407fdb56dc718c98425926831253978d727854":"e5ca84b907ac761a5e
68a9080da0a88a":"":104:"c8f78e4139dd3eaf2baef8aafb":"0cc3ede50b0d3fb9ada11300a3239a383c98f968ad65266
d57a195bb18d3e568fe6cabba258da4bee9e923c7c838e06dc887a6c49cc1453ea6a227c6a83e651a8742e0316cad5efc
93739393e3603446b5c920a206db1434adbb8ebde4d1a7a8699c7f6c61b2d57c9709b564338423b4f526d6c157647a6
c45da9dd521061f05":0

AES-GCM NIST Validation (AES-256,128,1024,0,96)
#0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"e35dcea17cbf391491ae5ba6056d0dd13b348183474dd4b
614742751bdebfc32":"5213542beb044910d7fdeec8bb89de93f350760e493286eaef1140485380d429f74a4279c1842
a5c64f3ca3381cb5dbb0621de48821bded650cb59703e0ca88f4e9c3d15875f9dc87d85ba7e4bae9986ef8c203fce6f0ce
52c28e3a93befb4cc4ba3d963d2283cd30f9bf6ab99d92f2f4f3aff0b022f1751b89d43ea10bbb28a":"fa549b33b5a43d8
5f012929a4816297a":"":96:"afa61e843cee615c97de42a7":"FAIL":0

AES-GCM NIST Validation (AES-256,128,1024,0,96) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"844c50ddc0ac1d9364b21003287d6ae6360d12bbb17a853
51362420ee4ca588e":"3a3bf4ccaf05f7c02f5e158dd2c5cb08c6aed4b1ba404a6d8ef9a0737fe2f350b3e22188fc330ea
63e35df82f996e3cf94d331c4246cdb25bb2c409762e05ddc21f337edee51b64f1766ad18f520b3f34735b24278d9d647
c533a743e0c1e9c81e9dee975cdc47e8582113fd250ef59353605b64acb7c025a97854c1a5c03237":"2f8512bb7e214d
b774a217a4615139e1":"":96:"f1da1cebe00d80eb4e025feb":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,1024,0,96) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"2aae1aa047a20ed2d6d8336d923864cee9404f924031ae327fbfe2d293e1d93c":"8e5b6b9e4e7d01de9a919dd33c0c1eb94dcfebf28847c754c62c1c00642d9e96f15b5d28ad103ff6969be750aadfd02fc146935562c83ec459a932a2fd5fda32eb851e6cff33335abd5c2434ae4f5524d6bc74a38094ced360f4606a1a17096ff06604952c8ca94a9a6dc4a251e13b0e0c54bd8a6dff5f397a1eb1cf186fa518":"3da9af3567d70553ca3a9636f0b26470":"":96:"e1026b3d15d261b2fb47632e":"58c52ea9f3b162511160eed1a68b6f52b3c4f5834af728de97a3d9e4ba337b29aad12636003cf5be9ffbeae0f383f7cf32f645a8f6fc5cdc1cde91c625c69a92bc434ed671e52a0044a48f3fce55cae49a7d065c2a72603a7efe58b5a7b18ac500d1a51420e820357e7a439b1c02198ebe3d4e62d5573a3aa5f40900a21e3b41":0

AES-GCM NIST Validation (AES-256,128,1024,0,64) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"f3d69208cb0d27474e9a231cd46eac7c1574fff950c48bbd1ba03fad16f563df":"0d1f06eef5e8f2c81d1a73bb1dca93c22cfb6e40e9948bc75b0d84830fb9216330424f580b89050c3fb3f620eca8f9fd09fb86d2e8b3a0869c6022d8a705fc280d66fd16d3aba7395d6be4bed44145d51d42d56285f3675726d62d94c081364a6d440511de83a613c598b03078e2ec7648c6302defbbea66aafd33e1a4b1686c":"b957f05921d21f2192f587768dc12b4f":"":64:"322374fbb192abbc":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,1024,0,64) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"cb2cdeb17fa6bcb006c7fc60858a12a411804464458db351957e8caf42f1ee6c":"296504131354b2c1928982f12d408ba2377f2d4bbe87e4c69f92a15bf6003910a43bda6c8929df66b3ab1d202a5258cad199f32f36cc30d2dc06199c2a52f7ccadad1fce50123c5f8434dec57cc60cc780263d7aace8f59cc8a6c54bddbaded3adb12ae2ee0bacf6a8da635ff85b51a4e8a1b3dc404863b90059de4ad0f158dd":"31bd7c971a6d330b566567ab19590545":"":64:"efc5a1acf433aaa3":"FAIL":0

AES-GCM NIST Validation (AES-256,128,1024,0,64) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"f94170790fadab3240df568197f9d6f6855afaed8d07eceeaa2380121872529f":"ed231b78db082f652bc6310c396993b52de804a82464fa3fac602a1286535f59c67fc2b1b420c7321eb42b971edde24cd4cb9e75c843f2ac6fb8ecdad612d2e5049cf39327aa7a8d43ec821161c385f3fdc92284a764a5d1cbae886f07f93017f83a105bb7c3cc4fc51e2781516a2471b65c940ddae6b550ad37b35f53d7cc64":"2f9c0647a4af7f61ced45f28d45c43f1":"":64:"ab74877a0b223e1c":"1cb5ed0c10cee98ff8ecfa5a1b6592391bbd9f9b1dc1ff351e0af23920d546b5e27d62b94daabd32f7f96a2632dc9fd7c19bf55f3b9b7cd492e76f4d6b0f5b437c155c14a75e65bfc4120bef186da05e06a2fd3696f210292ee422ddbce6e63d99ee766b683631394387 33c5e567177f72e52ef2df6a7dd33fc0376d12ec3005":0

AES-GCM
NIST Validation (AES-256,128,1024,0,32) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"797c0091ff8787fe7cd0427c02922620e7f6fb71c52ddcc03a9f25c89ba33490":"2d3efc8900315c3691a8e3c9de3319d4deaf538fcf41aa0e295b861d0ac85baf56d149a6437747dd6976f44016e012b88de542fb8e5b9e4ad10c19deec4b7c0b69bc1b2e33d44a981ded66127dea354b072010b8dc24b85ed2ffeea3b9c0e931619dbbf22677691f0d54fc03eaa162e0ab0d760ad41021f67057c0d6ac19ca8f":"69d81c73008a6827a692fa636fbab8bb":"":32:"be2dda5c":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,1024,0,32) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"90ce1afb5500489b9edbad987f4009509c847b3e55cdf0c764ef2fb085e3d033":"98482b54edce2bac1cd64d44917dcf117ebfbfe26ad17a9b263447028304f1cf5a69559c05b5d833420f4fddb6e308277d01eb4b3235f1c4b47d33d3899325b55e7be19d43187a5b1b1354ce02a529b3df1c13b4883902ae9fc565079dee825e705f3e580371e4fd86c3b0d31bae98adb529901f346ca07127314152b4370edd":"e119e166471ecf44bc3a070639619931":"":32:"b2f54b3a":"FAIL":0

AES-GCM NIST Validation (AES-256,128,1024,0,32) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"29264a90f114a800c0fc3247b3bda00981a12a8f85cf3a19ea4c7ffdd005f4bb":"587c8e53ab5ae8c31e16160b4a41d88798e27f4ad61c573c023c62d4dbb3952eef5026ad7b453fa9e0694347ab8fe50a6cf20da566202b81e325cee9c07ab2d4d53ed45b3ec2d2135936515f8a24f2a8116807dce9df3c44edf64c32647145152ff241d9e018e4101e400af070192dc3b498b5a213d265b4cfc8c8d4d7deccb5":"cf296aa43cb7b328e09c8975e067404e":"":32:"56015c1e":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,128) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"84ff9a8772815b929d55f6052c0354cf3e02bcc8336fcfe5794952b4c45d5d96":"a87de56d49725a1625baf12fd15931fe1a6783dce5d1e744eba108f45e0c105d8141dc027d0e33ad7efb6752b43729715e2f3e2c42ebdab4d5f72f886bd821c4372244699ddded99a63dbe7763a5a3bc21cbfc253cdc2514eba2a4f54e24dca7c207cb3f6ae80153d77fe0641f357d5a073dcd425c38deb77c45f27427345516":"5c044a66e488b853baf479f7dee2aadb":"00304e3d40cbc6d2bee0778462884f4ec047a8c74bb3dd7e100f2b9d0e529fd24730063986117b56ca876b208a3691425ac63afc3d504ccb499c76622eade09717023fcb7d956b01ce24a3e53cb5da472be3fcf5b278b5d9e377de22fab75bc74afa9670f5fe9691aa0ed77e43f6abc67a61ec409ec39fd66ac0307bf195f36f":128:"72ddd9966ede9b684bc981cbb2113313":"aadb8537309940422f67ca393aa6182d67fe7c52092538a15e98a4254f0a9087c7f10903d5e78078c2e55de914dec8b6b35cb720e3e55963c0ac9901e44b83a0e7c5b2d3f002aec0a4a08354febe47b2abb955f2a21107626ef0b8e1e099650812a6fecf36908fce2d078c2735cf7c2b970a309e5c6d6ff29c26a05720c57105":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,128) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"b5ca3991d0160b1729ae1a622dcf4b03b1f4ba86150bd66bf35cbbee9258af10":"62aad5854a238f096bdde0711ac6f5763e7fea29db068ea8c911f17ba91e6d7807883e6fc5ba7db17af33da2b00973008a3425e65cc786ce1b97360019ee2cef74563d54752be436b905705b507c3d62689df4edf0356d26b693eb43d8a2a927a9f3866b7e0e19e84a90447bd6f47e31070fa7c2a71e3f78229ee19fa47e848f":"f8402184d1cc36df07b68ecb1ab42047":"d378cfd29758bcbd21e26a324239c42c992941b3ad68d9f2b3d2def3a051fd172ee882562970ef59798ff8d9eb5f724ff17626156f4cf5d93e41ffef6e525919af6194ea9bbb58c67563d3ffd90e5a6e2a3a33bd1fa3d55eff5dba7cd439d571f7e08014c4780e3d10904ef22b660897e78258da20b2600e88d71c35ecb6329a":128:"9e8b59b4971130557aa84ec3ac7e4133":"556dd32edc0af3c64186fe8c000ddad1516cd14721c93c228e379d4f87e32c79e734539cec930322048f34a2b34931c585d44f09966caf187ec4b9244c991a8a5f263e9da1d08d6086e52535afdb36c7662307521cbceb9ecb470a76970243723fbc1613b6ebbcae261ac2f1936e66ce29ec7350b2e6b2f73a910ade645154f7":0

AES-GCM

NIST Validation (AES-256,128,1024,1024,128) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"df867d1dd8a287821a54479cab6f88636d2aca30e1bf01a5dffc735e17590356":"6517272cac85d7f38902bcb4b96a0c59c4bdc46bfefa6ebacd7f2fb1629b87ca91de2ffefc42ce3cfd34dcbf01b3f7cadcea3f99e6addf35d36c51f2ceb1f85c1f56a04ec9c9fff60cd7fc238674992183ea3de72ef778561b906202b7b83fe6562a0bca9c1e0a18638e8685b998b4192f5120435809ad6e93a0422d00725262":"35019826c51dd1ef07ff915d9ac4ea96":"0375ed93f287eefe414ab2968844bd10148860c528dbf571a77aa74f98cc669a7fc317adc9f7cf2d80dda29b19db635b30a044399f3665b6176ed669146d28f5ada03b3d32d53fe46575a8afcd37f20386d9e36f7e090b4fefadfab7f008e02f1b5022c0eeb81d03443a276eae48c038ed173631687d2450b913b02c97243edb":128:"e49beb083a9b008ae97a17e3825692f0":"723be39bc13adbc48c861b07753f64fac1ae28fc8933acba888b6538721df0a8b91c040a26522fe0dbb7335d8f63d209e89f7cde23afa9ca3c584b336d63a91e07fdd8808b14c3214c96a202e665bbaaa34248ff30348f3d79c9f16e66ad6c5903305acd887a89b6244eb7c2d96e18b13a686de935bf3821444ee20f48678be5":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,120) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"0e8e9ce6294b7fbc534a96bdd060120976a6e08315d2ea73ac61d085cd462a44":"9855f186b51358f0e2111c06bfaaeaec9bf95c55e246375c614fad9883d86c82a20c86538dc5f42a0ea69677d59a20c5112d15d2a8396f12096242ad5d7b838d16ee0679fc4017af75bc15e8ad2f77b0e802c864031cbfb0bacd95c828d1db4b7bab0713619e9e5e8fe6902aac7a9e6c42eb05f5b156f7e663ee43e6fdb62480":"4edc6be20f904b4789e5bee0a80a3fc8":"db28ce076b360816cd1e04b7729f8ab080e0a07f35204350f3bd056945aab8638c0e8311ab056f3e5debdbfbb03fae700770264faf73e0f3a05a5812aee84ab613c82f4a76da276250675f6a663f85e2c26d4f4a8666a7f4cedaffc1a7218dec11ca4e72b8b5d5b620d1efbd3d3b94a5ae0d118b9860dfd543b04c78d13a94c3":120:"03cfe6c36c3f54b3188a6ef3866b84":"e10142f852a0d680c983aad2b4609ccbd35ff61bb3eb66442aee6e01d4cc1cd70f45210acbd506395d6ca0cfebc195a196c94b94fc2afb9ffa3b1714653e07e048804746955e2070e1e96bff58f9bc56f3862aaa5fe23a6a57b5e764666ddec9e3e5a6af063f2c150889268619d0128b3b5562d27070e58e41aadd471d92d07e":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,120) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"886c77b80f5f3a21c01932685a540b23629f6d41d5574fc527227ed0bdf2e21b":"53a17d7b69f607f08676d6f6dd4e8db08e01333a8355d8c87616e84cdf10ef5b041fc6ddc3f6a245c0f534c2b167064af82f45e4702a5e8dede59579fdecf6713353392433950c9b97c38d9ee515ac97d0970ccf03981954540088567a30941bb2cca08cbed680500f8342faa7aebbc6c143e2ea57ba6b4ac1fd975dcc5d0871":"5ec506edb1890a5a63b464490450d419":"05b8d820c9f439d7aeae5c7da0ee25fb0dad47cc3e6f3a47e8b984e856201546975f8214531fc3c2e504d2ac10fa49cb948596b9a8fab01b95c49d6f04d1589f93b77b899e803dd20e1f00a51c0b5953e85be639109b14b100e35ca26d84ea629964b0db8260dfa5a150a66261bf37e79de2ec49e9f1b082a7c58ecd3d39b6c9":120:"ffdf56e1c1a7252b88422787536484":"79ee27adfa9698a97d217c5010ec807806feda37db811e398c3b82abf698aece08561fffc6c601d2691738e279eeb57e5804e1405a9913830e3ba0d7b979213ef40d733a19497d4bb1b8b2c609a8f904e29771fa230c39a48ebb8c3376f07c8013fff6e34f10fe53988a6ec87a9296c0a7cfba769adefe599ec6671012965973":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,120) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"5231ca6d772edd9ea2d251e22d7d455928c22474b4b44130dad57e6511fed6ee":"2767c808410ee132291585ea74a48ad3102f883f07d060c91c5f10abd37fe0996d2210dc490260238ae15f5d74c7be2a1e15d80db09079c520047f88488a7802857a3fc3b81d85a96949997430a880177880a31d4d0c9c9045247804f057a4f2756d6e40375a4a3187c4376d6bf573ce334cda1ed88d8a50db499e7cdb89d8db":"048698a4a0f

eabc1f336112e2794795a":"3a81b6b0b722899ff931cb73c39222d555b83ae3f8880b982593cbc1ab8be90d1ee32fd7df
e697cf24c95b7309d82c3fed3aa6b3d5740cc86a28174ac8f17d860ebb251ac0d71751c2ff47b48bfb0b3beb4f5149446
4cda34feaecddb1dbbe5fa36c681ada0787d6ed728afc4008b95929a1905787917adc95f1034fedcd817a":120:"ba61ede
b7b8966188854fc7926aad2":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,112) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"5a3f516a7898e04e5da4efd6c7c5989b77552d195464620
c2b35b9a4fda29cce":"5cc28b61ae97557774bdcd7ff653f4aa349df68d53c7e5a65263883ef1fe224ad40e86bffc2d38f2
8a2ed9ae1fc08563e2a1e46246106546eb8e6064c06baa0046fa137421734b7f0f94656a4f459d9d981717557d843700
d116b6e5e2dd3af5f67c34edf31b40b71fd3c6f2475f9310feb70bcb973be52d41e86792c49d54c0":"9310af6974890c0
a0364231f9cc8103d":"2103af8356bcb9dfc2a4f1d4ed09cbcd8e1990d23865605e19f87feb50bf8d10d0257740e5557a
9297f0499c01e29a1a513ca18e6f43f7406c865cbe3951a7771128f3110c8da3bd6963689019445495528 42a1f6fd96cc
681b45da098f3c1acb3d237d2363285f520d0b6714b698790b7660c52ac84a42c9721ac7e9d38a2ef":112:"993fc8e71
76557ee9eb8dd944691":"FAIL":0

AES-GCM NIST Validation (AES-256,128,1024,1024,112) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"59c9258554363d8a885fc0f5d112fee08eadfc7ce52a0e7e7
3e3d0d41d9a0290":"79c491411402ea7878e480519fd984dde44bce6459303bb76d4eaf97d4e345d1aafaa68ceb0590b
41cfed0f411b675d9344c7e888cccfc9eb6fe6b229d198f94ba516ee850ee7f078a4f5f32a23f92f72264e3a76a31ebd042
564315ac4f2ec0bb49ba6d08cfd2d3a6308688e39f28e3ecd669c588368cee8210edf5dbefb925":"77e51e89dc47bbcac
79cca21e81a61de":"25a6f8800a9b914c0ebf9a45d72355c03ee72a138eb81b2980f332645ce1d7aa4659805821866ae
e2b276e2c032776b4eaf36f93b5f9a72b791be24e31eff105ca6d0700e3069ee327983dd7fe1c7465d6c6d77837aff6905
5149988e7199847fad98605c377d997dbd40f3e2ff1a4f978a493684e401249e69540fbde96323c":112:"ee6d85d3f370
3b45adb4f9b2f155":"44ca68deed5478074adfddc97f06f44c08bf7bca4dee8707d621fc7396fe2efcdad0a167d1708a9ff
59ce4cddb86920bf1dbdf41b2109a1815ffc4e596787319114cad8adab46cf7f080c9ef20bcf67a8441ba55eac449f9792
80319524c74cf247818a8c5478ea6f6770996026a43781285dd89c36212050afc88faa56135fb":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,112)
#2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"5e9eae594cb54c8089330e4404ff79abb1c0841b0be5347a
14633ad1e1ff44fa":"32abc1eb6077555a85a0a6fd1c78cccca6c8b375842e2eb8eee45ee6c38dc0837443d16c647252e
8124639dd01c808ac5e857a25d927c2a75e2fa8955cad5beb5c206fc050cd933fc4621f5718936f01f39dd700ae1aee75
37cc595df8789c5d1a6e1e87b1c7a60e3ce5d57c80dd65dee3801798e1481b1963bcc78cc69f8c50":"0917b486da754f
48bb43ecc8766a7ce3":"2aa1ef2f91aeba5da10b48a882dbd4574df4e9157a18abf8cecd03e4176712ba171b6ecb0e745
841ff84e35063e47b08101afc44cfd9cededb913a82f00b9d4bac922f23a22f20064227039989640 5d00fa5271718eefb4
cd5fe7e5f32097766ebff36ff1898a1c8a1a01cc18e6121e470805c37ff298fc65ef2fb1b336d09fd":112:"92282b022e39
3924ab9c65b258c2":"FAIL":0

AES-GCM NIST Validation (AES-256,128,1024,1024,104) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"aaf03c3055a35362212b9b059931e7a24fc71e32bc9a5334
28c9dc31077f2ebc":"c0e12cdd8233878505e025d52427536be7b6bf1887d2dd20eac7092db80b22417a3a4ca83cdf5b
c5e36161be1ff9b73f7ceb297c6d07c9cb2a75035a5dc079e48283daea60596f4b356ca28c243e628cbe459f069709fe19

3394c9b1a31d8ccc5a3a4eba30056c415e68571a2c34bb5c32efff12e9aa483c4a68be5e76aba4cd":"7dfccd077b29e6e
d5720244bb76bde9f":"21edd1c6056f51fd5f314e5c26728182edcd9df92877f30498949098dcde8089eed84e76d774ef
8874d77125669a302d268b99dcd66b349d0271dde6f8cc94dc4f2df3787887b1173cad94d067e346846befb108005387
102854d9387d2c0fbc9636cdf73a10d145f4b612c201b46e1ff4465f6a7654ce3da5792daf9a27fb35":104:"6154c6799a
d7cdc2d89801943a":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,104) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"60c775971a9eac7950ed2bdd85bd60fe948ba04c419f674
3fb67f37557e46c6e":"8abb2e66a4d08074916056bb8e925551372f737f0e1b597c5d08ee102989743a273b29d728101
3f8b3aee2934399cb427370d70370ee86eb41584b653660c633506a53cae747826bb7d93909f069d5aacf058b7f2bbdc
58ea08653db857bda83a979fc22a4f126dfef7aac45177f4cdb802fab0c812fb35d12a8176ec21336d7":"9b92ad7079b0
de09c94091386577338b":"1f6a84b0df75bd99a2a64849e9686957c6a60932ebe898d033128be9b757e9890225925d8
56bfdc33ff514c63145f357730bb0435c65342bc5e025267b410af6fd388a5eca01b7efc87fd3b1b791df791bd47dfab73
6350d7b7f368b4100e04c939d5af957bab95ed502dac904e969876674602a0f0790da2d7351b686e46590":104:"1d6cd
4ab3914e109f22668867f":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,104) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"3b426e449337a14bc0663246ab61b671b523c9a3130c21e
d59c93fa6a5aa5ae3":"291bd5a00d71eb7d547b7c94e7030ba4a947418eaeb378a3bacd304b08c6f92f6958eaba968ac6
aa23e0512a2a8ad7c1ca2f8fcf623bfc1281f5b7b598c08d2aebcd447668b23238c5e338b4c2ac7f8fd381714c596ea3e0
c17aca4317a08563e58f0f52a8af08e078dc242ae54ee0fe3869f8c9687b004a4ded0aa27d8f4c5d":"e6efc96acd105fe4a
48d1ac931eea096":"0902cf7a0685444126369712ac47962bc2f7a3a5837f1b6190d9ab1adb4cd35e7f0892eee628b8e
07fcf2b598cebe1ec07d8c4823172ae66a135bb51cc71590707b691a66b56af1ffe38772911d11685da355728eaddd837
52d21c119d7b59f4c17c2403629fa55cd70cd331aed7b0de673c85f25c2e9e0267f53f0b7480c8ca":104:"ca4bfeedcd19
d301d3f08cb729":"bcef3f2fd101b828d36cb38530cf9a0a7a285ac1c55ee1069cc78466327e85887534c98a8891d579e
ffd832c0f7d6e7e822fb1eea85a39317a547591def4aeed6660872859fc9d1df9725d3c40e9ccaa900e0f1426a55d20ac4f
2e8e07bd3bbc687f8e059ab93e7604c97e75ac94be1c8c24f4c4da0080a4d77953fb090cbb62":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,96) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"ceaf204ff504ea8e7fade1a2097f2b527a44766860447322f
a5ad346cd810217":"1c8e4cf6018211518494d46c2e0607fa42e236abc28d58f8175c530f84b1f030572f5f6a74cb5517
e1fb999a637d352afcbeadea9121e695675859b66b499a3a351ecba5226e58ebbb59fe12e359e4c89cd51c8703d4643c4
9921ae495801c73627df404b91e828e1d0e03ae09a39defb5aa5f2c8106953772ba0713d3261329":"cfdb8183251f4b6
1c64e73243594fdc6":"a60f3969fd1b14793dd1425aa0b1f742a4861e0b50eaffd1525cd209ba6d1252176763bb5bee5
9aaa55f92341cdc0705899aba44cf0ec05cbf80274ebef65cd9507fd4224b25cac19610968d6a37e2daf9ddf046ef158ef5
12401f8fd0e4f95662eebdee09dd4a7894cc8c409be086d41280bd78d6bc04c35a4e8cd3a2e83be3":96:"9e45029f4f13
a4767ee05cec":"5cdc66b587ed5eebb04f42b83a6ab7017093514881c598cce332d74fa3fab927493ac15bff26835296e
080b5b45ef907c0529fc2f4ed2fc09db179ef598e5d193ea60c301d3f8d823404814e3e74de0e1d2417c963e9246c3532
01c7a42659d447376e7d05c579dd4c3ae51c2436407b8eff16ec31f592f04b8013efcfd0f367":0

AES-GCM

NIST Validation (AES-256,128,1024,1024,96) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"15652abe38cd09777bba21d0db04637f5737d3cb3922181
b9f2d07bfdafd327a":"1d6c153dec3b4738a09c9fbdfe31a093eb7ea79b8fa49f83e5e1f46893590f074fb171fb66e30ef8
87767014e3a10a3aa05da2bd50dd7b7936e1d7f6f31af9030e31e76bdf147f4396464db0f6a72511c4885c6c2305d3399
06e3c761a3249d7ebea3bf463e8b79c3706e684575550e964b8047979f7aed6ea05056c4b5840b1":"3a5e0d223ae981e
fb405566264e3e776":"cd755437cb61b539908e0cfaaa36c0123f8f17d1e6539783cb61d4b56cac3bc1e971c1ea558b1
2669b025cb6b9ad55991c6e2f8ee8b0b7901790193e226a0fbbfff7ff0bee6a554660b9f32e061b6c04bf048484ff9ebd4
92f7e50e744edd72d02c8fd32f87f9421bf18a5a20ebb4d9dbe39a13c34b7296232470e8be587ba09":96:"01a573d8e99
c884563310954":"162430c23f7adcf98575a2d9249b4b5cec42efae33776360ebfa6a19c8eee4bd6b07cbd274deadc329
2b7cdbb7803e99d9f67ccc5077f3ad5808f339a05b3213dbfd11377673d4f9b486a67a72a9ac8ea9ba699861dce0de7e2
fd83d3ba2a2ec7fabf18b95a2bbe2184ff7bddd63111b560b3afe7f2c76807614ba36c1b011fb":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,96) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"a43f6d07042a15cd49f6f52a2a3a67c6c2ff420d95bb94b9f
e03b287c3abcaf8":"b67e58c8b608724fd20aa097ee483bc4c804490cc79de635170944af75c87ae0ad8261365c1dc80
d852553bcba18da9fbc3fbe61d27550a03003ef0c60202054626655509a9e1ab54677e537a4e761df011d6c6dd041c79
5446b384161ae9eab441afd24d19b58eb4fe5116cd7b11b751ebbd0a2adba7afc380d9d775177099a":"3b6fad21f0034
bba8b1f7a344edf7a3c":"2e01c0523c8293fc51388281dccdb8d0a2d215d729289deb327b8142d716c2bb849e9476545
b82f3882ba7961b70c5da2a925ba18b6b121e9215d52ac479c9129c9cd28f81584ff84509d5f9dcb7eaae66911b303cc3
88efa5020ac26a9cd9ea953f61992a306eb4b35bcd8447eea63cef37bb0c95c1e37811115cf26c53e8c5":96:"43470bc3
d7c573cb3a5230f5":"e1720d451fa7ab9db4988567187244b15b6fe795dd4fef579fb72e41b21aaa436d2e5d8735a4abd
232a3fb9188c75c247f6034cdebb07fd7f260f8e54efefa4f2981cafa510dd5c482a27753a7c015b3cae1c18c7c99a6d6da
a4781b80f18bbe6620bfc1518a32531017a1a52aadb96a7794887c11ad6bdd68187ba14f72a4b5":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,64) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"1f0f0191e18db07c0501dbab4ed952c5603a4cd249d2d8d
17e62e10b96ae713f":"aad40e7866c26e486b6f6e8eb14a130d5f88891bf0d09aa8fe32f447ab8dea7bee5d3eda4499c0
103a010483f2b64fdf1155499d31decf528c77dd7627884f9995c213cf7402143dbb7561d69c86886734260ac94ffac7e
b33598d25714228ef43f744ec1af2a87e789f1e5d6fff0fbd5082dcc49328f194e8f8a14a5bfc962d":"ab8be16b4db809c
81be4684b726c05ab":"a5a6e828352a44bd438ad58de80011be0408d410f6e762e3145f8b264a70c593476b41bb8787
5746c97de7d5fab120bd2f716b37c343608ee48d197a46c7546fafcdbe3e7688b7e9d2f5b6319c91d3881d804546b5f3d
be480996968dd046f406c11f0dc671be0421cbc8b4ea6811dd504281518bb96148dddf9f0dc4e2e2436":64:"d8bd7d87
73893519":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,64) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"a6cf7d83137f57f2310ee6bf31e8883952bb07ccdc12f516
233ed533ea967e5d":"83ab20698fd7573fd121976a72b45a7f03aad84702fc8ac73d6926eabd8a546895aeffe4ba81d11
7507e2cd37d58eeff71cc3afa8a4449be85f228ea52f6dc6395bb43c1c9f795343720841682d9b2f00602eafa4d4cbe297
bfc62467e526b9d823cc8eeecd9e5f8dbc2f65610663c6f37b3d896651b254bd60215629ade3b2a":"f17e37e73a28c682
366bfe619cc673bb":"0f4dd201b18e20230b6233e0d7add6f96537dd4e82d3d0704c047fab41af5faf6bd52bd14fa9a07
2f81d92a2ce04352f0b66f088c67102d2d127a9850b09ff6087f194a6e8ccaba24091feb303eebb65f1203b2d22af44e7b

e4de71f03e6f6cbadf28e15af58f58eb62e5bddfae06df773cc3f0942520de20078dda752e3270f":64:"74110471ccd759
12":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,64) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"b0c85ac6b3887639838ddca94c5c69f38115aa00122322c
8114642d12ea1b8fe":"0210fce418e7e2199cb8f899c81b9be74a630d00269755f882fc4db27632e99685cc12c426a75
03473646df1288d0ede28408be9add5713628700f8e2b2e27d7522520ed00ac47239084651eb99e7d03e1520aae137b
768f3144232c16b72158fd5da4a26a2525b9b27791bf06d1eb2e671c54daf64fddc1420bc2a30a324ba5":"14f68e533ec
f02bceb9a504d452e78c7":"796a46236fd0ff6572b1d6257c874038f870aa71cbb06b39046d0fb6489d6ae8622b51542
92ae5c4e1d5ff706daedb2e812533ae3a635d339a7fbe53780e3e8204924a5deb4b6856618f4c7465d125a3edffe1ab8f8
8b31d49537791c0f3171f08dbb5ed1d9ed863dafbae4ecb46824a4922862fe0954ee2caa09ab0e77ed8fc":64:"6fb0b5c8
3b5212bf":"5e6c362f7587936bcb306673713a6f1fb080783a20e9bbb906456973e529cfa0298206184509c30e1d3793
eaaa5d564edd4488f04311821eb652e0a1f4adaf6971505ca014788c8ce085ceb3523d70284ed2bb0aebeba7af83d484d
f69c87f55a93b3d87baa43bd301c4e55eb8c45dcf3e4612535ea1bd5fdb4c3b9056d0cae9":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,32) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"e61b1a6b40e2ab1245ff65dcfb9948318ac4fe55e9ed600c
ec301dae32ae0e93":"8d67fa9fcf078e421cb63abeb25dba739ab0e09a091dd06b0c616e1e888f350edb2d73a42f57f11
5266ea20c7f8fc143ac746649612df06a5e29b4a15934dc049be1ab49d018ab86c4f37d8c3d9c714f038029e74d8ee3db
e61d81adc63712ea413b37f7604da12107aa1695d9b0981e5a92cdfaa5fbda0e31b22c6fd6f3b499":"c356244b3034d2
88e4d4fe901b8e27c1":"bdcfeb09d5b97bab05a7acd9849e7de2c5beb7a4dc573c7e1c1d0c0409245a6584023114fdcc
6413c800ca16847bde750b27c4d590248e2ce457c19b0f614f6aff4d78d4a19b3251531e5e852fbb05d09412cc1ff8988
d1955ca6f5fe2d820f20a7642e3ae69e8122b06ba0918e806400b9b615e1abe6fdd4f56a7d02d649083":32:"86acc02f":
"7c73182eca97d9617abb478a6ce62e3491a7e9951981c89c3071b161a4c80440614c3f24d0155073e28dcccee96bc83
03dab4901ef77318df522d16d9da47770ef022395d6104cd623d93d67090a27507fc8ca04157e7939e639c62cd0e7d8a
472314833c0eaa9ba2fd54a25b02854e3bff25cccd638885c082374ae520ed392":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,32) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"4f5a02e9843d28c8c226ed70d44b8fced8fb757ab6ece4d4
f06e3c3cec79e44f":"3ec13950d329f24074714c583bdc35686b811f775b76b0a8fcfa66fc56426c9d022f8ab0af38f8d2
f71a068548330cdbe891670181ed7491bf40c739ef4dd93689fd35929b225089d2b151f83d9b3cd76730061114458676
7354c0491112c205409f3168092d27f9b9f433afb79820a2811984d48e70c1fb2a13bbb3ddbc53fb":"099e5d9aae89fb6
391a18adf844a758e":"ad93e8662c3196e48cfdb5aa3bc923cd204151aa980cbec78f0d592b701f779c1c49f9e8686d7e
2385a4146b21a643a59c18c8b82214f42560bcd686fad7c7c8e8c1944ce6b20ec9537dd14b6cf2592740ca112f4cd5822
50d69f240d3e957040e1f7e19c60b3c8f2bd00cb666604c38946eb9b2f17336d281b4794f71e538a2":32:"30298885":"
FAIL":0

AES-GCM NIST Validation (AES-256,128,1024,1024,32) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"1cdb218e0bd0e02156e5b48182990f778889793ef6018a8
928e61164ac047c8e":"4d039618a0eb640329f90fe97de18bc928fc3fc7a0db42c97774bec2e882e872fc1097c8319f78
37a16516bf387b1bae321c565e8fc1cb8480f051158e4685f0adba310d2c6253bc1300403cbd3f7ddcb2796a69f8bf9e7

3d47aada9a02673c1a3d5ecdac838abf22b385906236529a1b7dd5b8af2611a04cf4f83b15ba41cfc":"d2ffbb176f86bee958e08e5c7c6357c7":"bc580c4223f34e4f867d97febf9b03629d1c00c73df94436852cafd1408c945c5474c554cb0faf2bae35d3160c823d339a64ebd607cf765fa91f416fc6db042bc2bd7445c129b4a0e04b6f92a7b7b669eb70be9f9b2569e774db7cb7ae83943e3a12d29221356e08e5bf1b09e65f193d00d9fe89f82b84b3b8b062e649163dc8":32:"1997daa9":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,0,0,128) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"dc1a145c18bdbca760f35eea0d4a5992de04a0615964ec8b419c8288ab1470f0":"":"7f8368254955e1b6d55b5c64458f3e66":"":128:"8ddaa2c3ed09d53731834fa932d9d3af":"FAIL":0

AES-GCM NIST Validation (AES-256,128,0,0,128) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"7b4766d3a6615ee58b390daa228ae7a541c46ce80a1efe227cc43cb777df3232":"":"274367f31ec16601fe87a8e35b7a22dd":"":128:"5f3a757b596e06e9b246ed9bac9397f9":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,0,0,128) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"d19b04055bf6e7ff82e89daef66c9d8319ab25f9197e559444c5729b92c4f338":"":"796efaff4f172bef78453d36a237cd36":"":128:"3b445f38bf4db94f1a9ec771173a29e8":"FAIL":0

AES-GCM NIST Validation (AES-256,128,0,0,120) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"7ca68e300534a90a7a87ca9906e4ac614a6aa51f769b6e6129753a4f83d10317":"":"45e6b23f8b3feefd4b0ea06880b2c324":"":120:"6c0a1c9c2cf5a40407bfa1d5958612":"FAIL":0

AES-GCM NIST Validation (AES-256,128,0,0,120) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"a2b7cd693239bbc93599d3d12c9876e7303b227b8ae718e2c62e689e1fd62903":"":"548c9c8fcc16416a9d2b35c29f0dacb3":"":120:"3aa21f221266e7773eeba4440d1d01":"":0

AES-GCM NIST
Validation (AES-256,128,0,0,120) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"156b854beb0c276a5e724f5da72f0d1ca4ae7cbd5f93a2257d95c2e5bfd78ad4":"":"a5129e2530f47bcad42fc5774ee09fe7":"":120:"6bb09ed183527c5d5ed46f568af35f":"FAIL":0

AES-GCM NIST Validation (AES-256,128,0,0,112) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"d824330c60141264e1f709d63227a9a731bcc42b4adec1d8f0161b10b4fdb2ab":"":"c5afaa45312c64ab3c3cf9d6c4e0cc47":"":112:"55952a01eee29d8a1734bbdf3f8f":"":0

AES-GCM NIST Validation (AES-256,128,0,0,112) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"b5517589948d8aea778df6fd66c17a170d327f69e504f0a4bd504c4286a9f578":"":"6404b111c6289eefa0d88ed6117bb730":"":112:"637f82e592831531a8e877adfc2c":"FAIL":0

AES-GCM NIST Validation (AES-256,128,0,0,112) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"f6137b2bcbd327fbcc7f313efa10f6ffaed30e4782e222e1225c87103fcae905":"":"3b87b08337a82272b192bd067e3245ec":"":112:"1f2dda372f20ffddd9dd4810e05f":"":0

AES-GCM
NIST Validation (AES-256,128,0,0,104) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"b5e70d1b78e931abf44bba3f937dbc344858516a8a8afe605818dc67d0c3e4c4":"":"58e70095c6f3a0cda2cdc7775e2f383d":"":104:"1763573f7dab8b46bc177e6147":"":0

AES-GCM NIST Validation (AES-256,128,0,0,104) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"90de0c047d1dd01d521f2dedec7eb81bc0ace7a5a693a7869eaafbb6e725ad7b":"":"d565c9cdfb5d0a25c4083b51729626bd":"":104:"78738d3e9f5e00b49635ac9a2d":"FAIL":0

AES-GCM NIST Validation (AES-256,128,0,0,104) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"c43e8dbeafb079692483a9fcbab964b76fccca6ca99e1388a1aa9bf78dfd2f02":"":"f2bd4fe0d30c0e8d429cac90c8a7b1c8":"":104:"ea7b52490943380ccc902ca5ae":"FAIL":0

AES-GCM NIST Validation (AES-256,128,0,0,96) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"13540919fdb95559e37b535a427efeee334309e34c4608459e204d931b8087e7":"":"c993c1802df0f075ce92963eb9bff9bd":"":96:"edfab013213591beb53e6419":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,0,0,96) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"2a7b2e07c148ff0f627ae28c241a395876bbed0c20f3fd637330e986db025714":"":"8f7e1621c2227839da4ea60548290ffa":"":96:"f9da62f59c080160ec30b43d":"FAIL":0

AES-GCM NIST Validation (AES-256,128,0,0,96) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"b3e7837a75b38ae6d4299a1ae4af3c2460dfca558708de0874d6b1a5689b8360":"":"05d363b2452beff4b47afb052ac3c973":"":96:"6b4a16d1ea1c21b22bdcb235":"FAIL":0

AES-GCM NIST Validation (AES-256,128,0,0,64) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"9df3ccd95f7570f6ecf5e5329dcb79bcd46cbcf083fe03aa8f5bd0f645c6a607":"":"774f4e70a7577b5101c0c3d019655d3e":"":64:"98ff89a8e28c03fd":"":0

AES-GCM NIST Validation (AES-256,128,0,0,64) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"1c7123e2e8d3774c8f1bdbb2272f19129e04f29b4351ae19c3b9d24e6ea1fe87":"":"99f25cebd6cfa7f41390b42df6a65f48":"":64:"8e14a0a4853a156a":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,0,0,64) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"490090323e9257517e2453469caa3414045cacb4d05d5cebc6b9c06fa6d19291":"":"c1beff1ff6cdd62339aa21149c4da1e6":"":64:"f998d7c08d609b3a":"":0

AES-GCM NIST Validation (AES-256,128,0,0,32) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"360e48dd38d9e7f5bf29a2994ab5b3c9c70247102d94049ae791850807a4c845":"":"88126c350dfc079c569210ee44a0e31a":"":32:"f2ebe5e4":"FAIL":0

AES-GCM NIST Validation (AES-256,128,0,0,32) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"1562b32e4dd843edaf4474b62cadd8f46d50461f5b22c9f1a8eae7367d35d71b":"":"af29fdb96f726c76f76c473c873b9e08":"":32:"13fd6dfd":"FAIL":0

AES-GCM NIST Validation (AES-256,128,0,0,32) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"d5160d0c98ffcb1c26aad755f67589000e2bb25fa940e6b1d81d780f421353d9":"":"1552604763453b48a57cea1aed8113f4":"":32:"660c5175":"":0

AES-GCM
NIST Validation (AES-256,128,0,1024,128) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"c3a3ea3a097c0c2b3a4cb78462d87fd5a8f348687c4150e9d3354b388ab13d17":"":"f77945979241fb3a454d8e3da193e169":"a69bac31241a2c07d3f7e331b77f662b1e67ccb81c07f52578b01f5785de9437f02eb7627ca7b9af09c1cb428fe93d6deb31f4d6dd2f0729f87480bdeb92d985de1aaad4bcebc6fbad83bede9a5dd1ca6a15bf5d8a96d4edb5bee1f7d195e9b2e5fb2221a596d69f257c18a143eda870e22d3f2ed20c9b3b0d8c8a229c462fff":128:"6b4b1a84f49befe3897d59ce85598a9f":"":0

AES-GCM NIST Validation (AES-256,128,0,1024,128) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"e1626327d987342cba5c8c63b75b4ed65463a2b9c831f4f9f80325fa867d1d73":"":"4e25800deab7ecec2a2311f8fb44eb7d":"ebaffd558f24dae03117c69ac4b2b4aaeaffe7e0e7599eaba678bfce23a9914dc9f80b69f4a1c837a5544cba08064a8f924064cba4d783623600d8b61837a08b4e0d4eb9218c29bc3edb8dd0e78c1534ab52331f949b09b25fbf73bece7054179817bc15b4e869c5df1af569c2b19cb6d060855be9a15f2cf497c168c4e683f2":128:"8faa0ffb91311a1a2827b86fec01788d":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,0,1024,128) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"938da64b837275b0c80c442bdf2301aa75e387fe65a775d

10a8ec840f62ff429":"":"dec6adeb60216cbb8a6c3afba49fa201":"4ac144bd95f405649444f01ab67ef3e4c0a54fdbd93
3b6ba00518c79db45c22c90030c45aadcfdb53ec8199be0cbb22dbb9ab938a871f4b3b0c98ed32590a051abb946c4272
6b3e9701f183b2092985e3457943a6350fbcaece2e6b111b179ea3fd10ac080a577a1481785111d5f294bc28519c470ff
94392a51a2c40a42d8b5":128:"2211ca91a809adb8cf55f001745c0563":"FAIL":0

AES-GCM NIST Validation (AES-256,128,0,1024,120) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"e2436484ea1f454d6451ad8dbd1574b208d7a3ab4fa3486
9299b85c24348b43d":"":"97040d2ec094fe1c64fa35b35b7451a7":"bc198677513ce0e66697dfe52b22315fa5d8f9204
2f34cc9f373a01f94607df1a599132f60af010ed9b5e52162dd7b162912b68b11700e08f5fdafd84d10f760fc05ec97c05
b83e55155194f399594015b90a19c04fb992e228940fe1b54ba59c4bb8318b33cc0df1cb1d71c389473dfb3eefabfe269
ca95db59a7bc0201c253":120:"2e080ba16011e22a779da1922345c2":"":0

AES-GCM
NIST Validation (AES-256,128,0,1024,120) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"7fb3fc72eb8a3aa5b102f90039f852cc3fd64f46915f5e49f
1d9e02fe9cc13b1":"":"f6120fea313362524917c53d90bafb4f":"60c2be7fbd15faf895fd19a9ce775fe2b183b45cffafe4
fcbf50d421bea97347e41a9418cfa129b2dda63b889a70063010215dbe38c37feae18bc31b34f31b726f22177f2b4b9d6
48dd4aa80edfd12dafaee10baa83224354432d1cb62ccabe38bb8448d162cd0d30e988d2e1a2458ffdafaacbdff9287563
90f66dc60d7ea45":120:"83de3f521fcfdaff902386f359e683":"FAIL":0

AES-GCM NIST Validation (AES-256,128,0,1024,120) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"697c96d80d0a3fa9af35b86f31fb71a17aed30ce841c7989
6bbc8863b3b3ee04":"":"3a5163ec7e007061838d755ac219855e":"de50c12da63232768d5eb9920d49683b5b7114cb
77448fa10b9d63552ec5d9c2eac94b375d11f944959f903bb20c696639b6e7f108ec1e873870098c631ddacb2c25268cf
c26d2a4cacfb7dda7383374c5456bcf4daa887a887f4293f8caa14419472a8bf7ffd214dfb2743091238b6d1142b116c2b
9f4360c6fe0015cd7de81":120:"cd4542b26094a1c8e058648874f06f":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,0,1024,112) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"66c1d9ce3feb0e966c33e3fd542ec11cc32f18c2514b9531
03d32abcdc72633a":"":"46fdb88fdde9b7d74e893802a0303256":"55d2f263d2e3cf0b390fce1dd1ebd5f666086f26e1
ce2f08002bedbb810ada3922c6bfcf6a6adaa556e9e326c9766f02b3eb6e278da2fa3baa7dbdb6373be3c6ecfbe646b1a3
9e27c5a449db9b559e7ea3496366b8cdbca00ee7a3dea7fdfbea1665bbf58bd69bb961c33a0fd7d37b580b6a82804f394
f9d5d4366772cee3115":112:"96ca402b16b0f2cd0cdff77935d3":"":0

AES-GCM NIST Validation (AES-256,128,0,1024,112) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"d7c949420dc9497232cd5810f316d11f9e85d36c430b594
3ba79836d88c1eb92":"":"7ef9788ff09cbeedd9569d49083a4097":"ca1de5cc3fcde2638eb72210e551e9c0e0a3f5570d
5be83a9a4406b545d854bf17e75b9cd0f4c45722fbd71319a317b72a8798485e9316a1c8102432b83bc95af42f6d5070
0ba68f6f2e19b6af609b73ad643dfa43da94be32cc09b024e087c120e4d2c20f96f8e9ddfe7eae186a540a22131cedfe55
6d1ebd9306684e345fd1":112:"8233588fca3ad1698d07b25fa3c4":"":0

AES-GCM

NIST Validation (AES-256,128,0,1024,112) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"6fe7c70815aa12326cdcbb2d2d3e088bbaaef98b730f87fe8510b33d30e12afe":"":"e0253bd1f19e99a7f8848206fb8ac4a4":"397897eca4856f90d14c3cdfe1ad3cba47e23174ae2dab7d2a6320898584e03bffa3ffd526f416d7b3c579b0f3628744e36eebb5df519240c81d8bbbf5c5966519c5da083ab30a7aa42deae6180e517cdd764b7f77d19cc1a84141817758887a8d7265e7e62279b9d33cd2f1ba10fd54c6c96d4b8a5dbe2318fef629c8e2af0f":112:"477b0a884d788d1905646bd66084":"":0

AES-GCM NIST Validation (AES-256,128,0,1024,104)
#0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"cbeefb3817cb02d617f385cf2371d52c8bcbc29e5e7a55cd2da131ca184c6e89":"":"f74156d6400ae46b612531848bffe18f":"1abe2ab05ceccf2391273126fe4a4426b94d2c3b97a7f1cd2ee6bb952bf4a546e972b5a1701d5ddb0e5bb7a248fcb47107a9fc77e4b9806b68a11850119aa239fa8be1370e3a2e1a8b168f7323afdfc4b8917d92570167848a56132d68876abc386c258a9233dc8a9eb73443b052e842c3d63e8b5369acdd038404e4e9a4b038":104:"0cb67cec1820339fa0552702dd":"FAIL":0

AES-GCM NIST Validation (AES-256,128,0,1024,104) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"e6f5f65ce2fc8ec3f602f5df90eb7d506dd771337913680ac16bdcd15c56583d":"":"9212a548c597677d1747e98ce6fb18a4":"55ca486c0183d0134925880d2e21dde0af51c4c77c6038a5a9c0497884e0aa4715bdb5b4bb864acc708ac00b511a24fa08496df6a0ca83259110e97a011b876e748a1d0eae2951ce7c22661a3e2ecf50633c50e3d26fa33c2319c139b288825b7aa5efbd133a5ce7483feecb11167099565e3131d5f0cb360f2174f46cb6b37c":104:"08d7cc52d1637db2a43c399310":"":0

AES-GCM
NIST Validation (AES-256,128,0,1024,104) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"0e9a0391435acb57eae2e6217e0941c79a3ff938ec6a19b8a7db2ea972e49f54":"":"27cd1d7af7e491e30c8110cc01392529":"79140d32bb32dace0779e2d37a0f744d6d973e99a279962b43a6c0af63772e8a0a21d5d9dd3c33d4b218cb2f6f24dd8d93bb4e1e6a788cb93135321ecfed455e747fa919b85b63b9e98b4980a8ccb3b19d50d735742cb5853720c2ad37fa5b0e655149583585830f8d799c0d2e67c0dc24fc9273d9730f3bb367c487a5f89a25":104:"fbb477dd4b9898a9abc5a45c63":"FAIL":0

AES-GCM NIST Validation (AES-256,128,0,1024,96) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"55a12eeca637654252e3e40b371667e3f308b00f2fd2af696223e4cd89e3fd4e":"":"8a3793b6441258360f7f4801b03d0b26":"f5810dc5f25e49bd6d94bc63c2494aa7a579a4056a25f1dd9b2734d0b8731ee52523edd54ff475651d45c213e1bf254327fb0e2c41a7d85345b02bcc9d27b08915d332e1659671991a4bb74055967bebbba6ecceb182f57977130623d5a7b2175fa5a84b334868661c1f450b95562928b4791759796a177d59ed18bbf141e2ad":96:"99230019630647aedebbb24b":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,0,1024,96) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"3d353f870a9c088de5674efd97646b9c5420b2bcdfcffefcadd81682847e5331":"":"f267fa982af5c85359b6447f9b7715ea":"7cf55630867af5dff747c8dd25bcc531d94a7730a20b6c03d46059ea93fcaa00d07ee17dad0e0dff814b02dfef0cbe00b37fd2f5f95ead7c72be60016f2934d7683fc1e47185c72

11c49cb03e209b088edb14e533dbcb792ab7033728904f7ff12381a236dba97894ec1fafcf853ab15fff343f9265d0283a
cef10168ffd1271":96:"9553b583d4f9a1a8946fe053":"FAIL":0

AES-GCM NIST Validation (AES-256,128,0,1024,96) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"d227c9ff5d17a984983056fb96f3991932ae8132377529c2
9238cf7db94a359d":"":"b8f6536f376a7efe0e684acf350bae70":"1cc25da31f90de7fa47ebce92754d3faa99f88d4e25c
cab45645c1acdf850d55d7f02f61a0bfdc3125f29259d7da8abef532fe0966c63d3486753c8a2cb63a39349a0641b2f2b9
526a03b97d58ca60fbb054c6c164ff2836688b0cad54df2b165bc082eeae660e768dde5130e30f8edc863446661c74da6
9b9e56de8ae388da0":96:"44b95a37fab232c2efb11231":"":0

AES-GCM
NIST Validation (AES-256,128,0,1024,64) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"b2a57ef85ffcf0548c3d087012b336c46f6574cf1d97ca087
bfad042ee83eec2":"":"3d580402d2a8dc4d7466e5dcb456be7a":"c2b9e95c16e55028794a63ef82d11fb83a2a75dc34a
81f238e472c33264534bdd54cd07d02a0ecf9019ad1a6d6c779f339dd479e37940486950f183bade24fca2f24f06d4037
b3555b09fc80279ea311769473eb0630b694a29823324cdf780d7d1a50d89f7a23b05f7a8c3ad04b7949aa9e6a55978b
a48d8078b5a2fd3c1bbb":64:"072d4118e70cd5ab":"":0

AES-GCM NIST Validation (AES-256,128,0,1024,64) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"63889ed5bf2c27d518a696b71c0f85592e3337aae95b5bf0
7289e4c5dfdc088d":"":"1ad534280a0fac7dce31f2ae4fb73f5a":"be1b9dabea33bb9443e27f674b27931c0fba699a33d
c86fab29e50b76a9441030444b465317bbf2949faf908bc1b501d11a5ea2042e4b460a85f3be5836729e523d99b56ef39
231d5c6d8ae2c2ab36ef44e2aa02a1f2c559c6e333216c7f9ed5f9b880a88e920219204c99a3ae8f90afd1396563bc59a6
91a93e0070b0b5fd90":64:"1bcea0ac2c1a0c73":"":0

AES-GCM
NIST Validation (AES-256,128,0,1024,64) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"94e3e2c17cfb6f52d4fdba3ba6d18bba891b6662e85df14d
7e61f04adb69e0e5":"":"8a80efb3bfe220526997543409fddb4d":"05da1b0f7ac6eef488d3f087ecae7f35abe3ef36d339
709dc3fcb5b471979268ee894c3b6c7f984300d70bc5ea5fba923bfb41d88652bdaecc710964c51f3e2ae2c280b7d6c8e
3b9a8a8991d19d92d46c8a158123187f19397ad1ad9080b4ffd04b82b5d68d89dacd3e76439013728c1395263e722b2
8e45dabf1ef46b8e70b5":64:"faa5c13d899f17ea":"":0

AES-GCM NIST Validation (AES-256,128,0,1024,32) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"fe5e479ad0d79dbf717a1f51f5250d467819e444b79cb3de
f1e0033c80ddadd8":"":"47ce838083fd070d8544c0ad5337cdc6":"98476bf05a18c4ff1b6024dd779c1ac06d838705a0
a83fe42bee5fc6ebf3b2a1a5049b67f4aabc8239cd6ff56504bcbad1e2498c159bbec2a6635933945f6ea49e5bc763dcf9
4f4b3643d3888f16105abb0965e24f51cb4949406124145e9ae31cc76535b4178492f38b311099df2751f674363ae7a5
8f6f93019653b7e6a6f0":32:"a3958500":"":0

AES-GCM
NIST Validation (AES-256,128,0,1024,32) #1
depends_on:MBEDTLS_AES_C

gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"27d4dedb71a8f68ca5ce2b9e56da772bf5a09b7981d41cd2
9f485bd2d1adb8d4":"":"7e6f0343c54539717a97b6c8b9f7dec4":"d386db78043f719b7e137cbf79a7f53dda2fe3baccb
ebb57d499f6eb168e5151f10081d76b72ae0f30165efbdda469e826f9246e59dbcad5c0b27691c00d6c192c24073e99c1
9cf8c142087c0b83c4ce2fc7ba1e696394e5620ab2d117d5dcd2ac2298997407fd5de07d008de8f9941a4a5f8074736a5
9404118afac0700be6c":32:"50fd1798":"":0

AES-GCM NIST Validation (AES-256,128,0,1024,32) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"5a7aa836a469d28542d0d24d3232fad266da8fc889c6b60
38b726d3da25f7b20":"":"9faf7cd805803e143ec8f3f13475efd2":"1006c707f608728b2bf64734062b12a5625062bcd
cb80a3ce2058352a2922d5e6fbe19681b4f0d79ad3c837f81e72f2fbf8df669894e802a39072b26c286f4b05188c708f7c
6edd5f5bb90b87ffa95b86d84d6c1c4591b11d22c772a8ad7f2fe6bd8b46be0e93672df2e8bff8ba80629e1846cfd4603e
75f2d98874665c1a089":32:"07764143":"":0

AES-GCM
NIST Validation (AES-256,128,1024,0,128) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"a9444fd176acbe061d0221fde3ddfcc4ff74e995d981a831
297c4cbda51c22a1":"c146ff5a988496cad7eced7a2ea471e0117d5d6bd2562c23ce9db4bf36d83ba3fc22e90486ec288
a627d208e0b2fd3b65f8301cf7fc41d97959981a95cd1cf37effc46db99b94b21c941c3613c26a10b1a6b7793f467d58ff
5134612230f1c49d7e1fcf664fe52fc6eca46273982f6fe729b009d90eb8d8e4a0b0dbe907b76da":"5714732145470da1
c42452e10cd274b5":"":128:"db85b830a03357f408587410ebafd10d":"a3cad9a57fa28e6f6aaa37150a803bf8b77e765
f0702e492c4e5ebb31ae6b12d791149153e469a92bb625784a699fd7ca517500ee3f2851840ba67063b28b481e24ba44
1314e8b7128f5aaccaf4c4e2c92258eb27310bf031422b7fc2f220f621d4c64837c9377222aced2411628018a409a7449
02c9e95c14b77d5bb7f5846b":0

AES-GCM NIST Validation (AES-256,128,1024,0,128)
#1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"686d3bd071e3f46f180611bc4ec8d7726fe72b6c617e7d42
b3339f53918c9e36":"21983ad66449c557263aef299da6eef8f31d576fc17ed2dac3e836f7c2ceaff3094b2695452680e1
88df10c174810efd1fbaa6c832baedce0b92e4c7121447f6461ac909b4302cdf658095b1de532b536faa4fb38cfdf4192e
b5c3fe090d979a343492f841b1edc6eb24b24bdcb90bbbe36d5f8409ce7d27194a7bb995ecc387":"a714e51e43aecfe2f
da8f824ea1dc4b7":"":128:"cd30c3618c10d57e9a4477b4a44c5c36":"9610908a0eb2ee885981c9e512e1a55075a212d
311073bbb2fb9248cce07af16ee4c58bdc8dbe806d28480f9065838146f3e1eb3ae97012cfe53863a13d487f061a49a6c
78ca22a321fa25157dbe68c47d78f2359540cc9031ee42d78855ed90e6b8ea3d67725bfffcb6db3d438c982b5f88d9b66
0f7d82cb300c1fa1edebb6b":0

AES-GCM NIST Validation (AES-256,128,1024,0,128) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"6fe81f15a02e2ecf46e61199c057102d160e6b5d447d4a27
5972323fff908c3e":"0b4ee0385e6665da8fd2ae47f2d0cf1c5bd395a3bb447047ab5a3ae0b95355bf83d0381119a8d4c
01acbe60cd7885da650502f73498a682fdc94f7b14f4c753226064fa15e3a90a6083e053f52f404b0d22394e243b187f9
13ee2c6bb16c3033f79d794852071970523a67467ce63c35390c163775de2be68b505a63f60245e8":"91d55cfdcdcd7d
735d48100ff82227c3":"":128:"cd7da82e890b6d7480c7186b2ea7e6f1":"FAIL":0

AES-GCM

NIST Validation (AES-256,128,1024,0,120) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"4c2095e1379389dc3810e8819314f5a2f87d1494213c5b1de1a402f7f4f746c4":"26ec8ebac0560538a948afbc18fb730e9a91f21392bde24b88b200f96114b229a5b57fa9d02cf10e6592d4dfb28bf0f00740c61157ce28784e9066ea3afd44ecf3a494723610cb593c0feffc6897e3435c6f448697ad3e241685c4e133eff53bdd0fe44dd8a033cfb1e1ea37a493934eb5303ae6ef47ce6478f767ef9e3301ab":"19788b2e0bd757947596676436e22df1":"":120:"f26a20bea561004267a0bfbf01674e":"FAIL":0

AES-GCM NIST Validation (AES-256,128,1024,0,120) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"be5351efc0277afc9759ec2464a22cb4401f7a17efd1a205e7af023c7ed30ee1":"1eca91406f338fc09c2988b1d7dc8c409d719300c03840a497d7b680cdd5e09b144903477f7116a934e1d931cf368af1fc2a0a0e7caa95475a3cd7bf585a16fda31eb3f8201db0216b37a1635c1c030836b3dd05ca5b0194388fa198e717822131d5d4318690ef82d35ac80b27fff19aec8f020dc6c6ce28f0813bbbf8230ad9":"c6b26117d9dbd80c1c242ad41abe2acc":"":120:"61051d6c0801b4a6b6ca0124c019f3":"95447aded336d6c20d483a6f062d533efed0261ad321d37bf8b7321b98f55c0f0082ce7f3d341b18fea29a72fc909d30cd8c84a1640227227287674a9b2f16a81b191ecf3b6232d656c32d7b38bea82a1b27d5897694a2be56d7e39aa1e725f326b91bad20455f58a94a545170cb43d13d4b91e1cee82abb6a6e0d95d4de0567":0

AES-GCM
NIST Validation (AES-256,128,1024,0,120) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"814c2cdfdeecf39d43bb141fbfc62dac44f7552c5e5dac2d4913303fc860119b":"0d3013a1d7132f685d001420daa6c7b643bc36b887511acc4588237d3b412c79e4ebba29c08248ad46c7239e8daa232b7483c9c4e3d1c0bbebc696401efe21f7fd6fc0525a4ab81bd9a893d5f7ab23b70ed07c00f33649b8a996a006de6c94f7793f72848793f4d5b31311c68aae1e715b37409fbe506dac038a0950f05fe82b":"0db3ade15cb0dea98a47d1377e034d63":"":120:"e62f910b6046ba4e934d3cfc6e024c":"374d03cfe4dacf668df5e703902cc784f011f418b43887702972dcc3f021bcb9bdd61ed5425f2975b6da7052c4859501eb2f295eb95d10ba6b2d74e7decc1acacebf8568e93a70a7f40be41ac38db6f751518c2f44a69c01c44745c51ad9a333eda9c89d001aa644f1e4063a8eb2a3592e21c6abc515b5aacaec8c32bcf1d3c4":0

AES-GCM
NIST Validation (AES-256,128,1024,0,112) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"1ae4541110f2bc4f83cd720b5c40c8315413d896e034b75007f172baa13d29ec":"5ea811e7fbfc0e00bf2a6abfac50cad9efd90041c5f7fb8f046a0fecbd193b70a2de8a774d01dd3cd54f848cb3e9f5152ee1b052ba698bebfba1fbbdae44a260447d6e6482640ae4d01c9cac3d37d4ffe9a0de0b6001de504a33ef7620efe3ce48ecd6f5b1b3a89185c86d4d662a843ff730e040e3668d6170be4cced8a18a1c":"83f98eec51ee4cae4cb7fe28b64d1355":"":112:"df47eef69ba2faab887aa8f48e4b":"FAIL":0

AES-GCM NIST Validation (AES-256,128,1024,0,112) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"20c9b662ec4bd13bf58d64cb0a7159b0e7fee4703af66292bf75c8bd6e42e8dc":"45b64f2ed5ac707890c0c1726adf338770ce6a728fe86bb372c4c49409a32705f881bc4d31a27c455c7c7df9dd2c541743523e7d32f88930d988857847f011be5f5f31a31e8812745147cbff5c1294d0fd4a7285db4833f22bf1975250da99c4d0dd2c9688d7f8001bb6ef2bc898ce4d42c5b78e74645b56ce992338f49d4183":"2bc0847d46f3d1064bbf8fe8567f54a2":"":112:"5a1bf25aa8d5c3fe5cf1be8e54a1":"9079d6275db076625e8474c2914fe483d413d5339202f98f06c3b0ef063d8f3d31029deaf7f9349bfec57e5cf11f46f02d5a6520c7992efc951adbbea6d08e53faeb10dfe8b67

ee4685da9ea4fe932551a65821147d06d4c462338e6ddda52017c2bc187fd6d02b7d5193f77da809d4e59a9061efad2f9cadbc4cd9b29728d32":0

AES-GCM
NIST Validation (AES-256,128,1024,0,112) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"0a1554db37f2e275732a77e521cbd8170729d8677a85db73feacf3c66a89d689":"5421d93b7e6e0091978c673df4f3a406aef5f13eb5e6f95da19b0783308cbe26d4fd6c669cc4a9f069d7e62e4c6fad14b80e918fe91556a9a941a28b3dbf776a68ac7c42df7059b5ed713e78120aec84e7b68e96226c2b5e11a994864ed61b122e7e42ef6cfdae278fadbae1b3ea3362f4e6dc68eef6a70477b8a3ffcfba0df9":"b9194a4d42b139f04c29178467955f1d":"":112:"05949d591793ca52e679bfdf64f3":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,1024,0,104) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"3ab1d9bb571c4bdc9f3ef340914bddcfe0c8e7718d4a2530334372cec86e5fcb":"80bcea307e009745724d5f15d21f3b61a5d5a8401530346b34a2adfa13e3e8c9c9327d6fad914b081e554fbe6c1c6fe070b566620e559555c702c0ab5becf61ea1d9de64351ce43b2276ef4e20b5af7ce43db6d21286af4e740ef00c6d790705afcf0ee4850fffc12c662f2bd8212feb21db31065ab8f717a7509c213352b869":"6a5335901284dd3b64dc4a7f810bab96":"":104:"04b8e5423aee8c06539f435edd":"36b9602eee20b8f18dce0783cd1e01a799f81ae0a1ce6d293a26c62f47e7dad85c8446697cc09c81d3d9ead6f9e55c4147211660c8aea9536cc5516e9883c7d6854be580af8cd47ba38fa8451f0dad9c904e0e7f9997eff7e29bf880cd7cedd79493a0e299efe644046e4a46bf6645dfb2397b3a482a346b215deb778c9b7636":0

AES-GCM
NIST Validation (AES-256,128,1024,0,104) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"7dddbd5657e22750bfe6baa70a1f4ac46c1ef8bee573a57cfcef50b66f85e593":"2bf5aba83a8161b9d21ff29251fb0efa697b1ea9c1b3de8481d5fd4d6b57afda0b098decdc8278cc855f25da4116ed558fc4e665a49a8fff3aef11115757a99c10b5a73b1f794f9502186c13dc79442f9226bbf4df19a6440281f76184933aeae438a25f85dbd0781e020a9f7e29fb8e517f597719e639cbd6061ea3b4b67fb0":"fcb962c39e4850efc8ffd43d9cd960a6":"":104:"1d8cdadcf1872fb2b697e82ef6":"FAIL":0

AES-GCM NIST Validation (AES-256,128,1024,0,104) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"6916b93b2712421f1f4582de7ec4237c4e42e2b32c7dced2f8bb5bd2e0598312":"3739cca20279a36ddb857ac22beae901a49529b3182463ab81a7c46e437eb0b0571e8c16f7b626ecd9f2ca0cd83debe3f83e5d58ed3738899f4b616755eb57fb965208f261736bdf7648b1f8595c6b6a779768115e3077dfee7a42d44b555a51675fb1ce9961d0e21b2b9b477c0541184350e70decf7c14a4c24b8a6cd5fed8e":"b4d9248bb500e40de99ca2a13e743f1c":"":104:"090d03446d65adcc0a42387e8e":"0255be7ac7ac6feb3a21f572f6a593cc8a97f17af7064c80e478f4a6c469cf94d604bc014b003bf284d216161a9c8a493af43c6a0d8caf813a9e6f83c7ed56dd57543876b11f76aa2be80dcd79d19ac61f00fa423ac2f52fae7a8327cd91494ca4116feb735980ad0a4b1445cb7f38cc712b8aee72179e65b97fca38694e3670":0

AES-GCM
NIST Validation (AES-256,128,1024,0,96) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"b751c8b724165009a8bd97a9d2a0e22cae5a95c4743c55e

eeef0a6fe7d946bec":"e8546a5af1e38114822e60e75563a9399c88796f303c99c69d1f3c50379da81e1cd5b5a4a721e2
3c59da58ea4361b7ff58408e506a27fea24f9a235c6af7f7a5bd93fa31e90edfc322821c08d6324134830b7fe160b4a3e6
d27866a10e6e60762a31618ef92f5c67ccb1deb1f1b188f0e687165e7c366c7418920df4f4fcdcae":"160c50c0621c03fd
1572df6ba49f0d1e":"":96:"9fef9becf21901496772996f":"175fa6b7cd781ec057ff78ba410f2897a920739b5fc4f04bc
9b998fbc7cc18e327ad44d59b167e4627256aaecd97dc3e4a7c9baaf51d177787a7f4a0a2d207a855753c4754d413489
82d9418b6b24b590632d5115dc186b0ba3bec16b41fa47c0077c5d091ec705e554475024814c5167121dd224c544686
398df3f33c210e82":0

AES-GCM
NIST Validation (AES-256,128,1024,0,96) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"0faf32c22c2a4ee38fe4b5ce08f98fdf6f83b5038dcba5ec83
32b3eeb5c710c7":"8a556cc30075753c6e94c2f669bca2058ff6abcbffffc82da7cfca0a45af82dfb4cf487ceb4ede72be87
ee4c8b72db1e96459de1dc96721464c544c001d785f2188b9fccaec4b1a37970d38b326f30163d2fdfdf8a2ce74aec55a
bcd823772b54f8081d086a2e7b17b4086d6c4a5ea67828ef0b593ea1387b2c61f5dfe8f2bb0":"04885a5846f5f75a7601
93de7f07853c":"":96:"0c13506ed9f082dd08434342":"FAIL":0

AES-GCM NIST Validation (AES-256,128,1024,0,96) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"0dddc3d2f82bdcdbc37648a6b9b416af28753740f8e998cd
1a52a0b665369f1c":"07bf84b15b21951fd22049be6991a672503ae243b8d285fb1e515e1d2c36bfd5b0d0bcce85791f
2cea8f616aed68a7d9cf4eaf76418e8b1ec27751de67cbfd9d9f7905b2667904f10d598503f04c04ea00a681ff89a9c446
d5763898430bd7a9dfebfe544e3ed3e639b362683a651e087626ffa63c0c2b3e0dd088b81b07f75e":"0a93b883cbd429
98ae2e39aab342cb28":"":96:"5c37918edb7aa65b246fd5a6":"ff7b7b2f88b8c6f9f9bad7152874e995eea0ff1ce1ecd9b
8d563642a37a31499f14d70f0dd835b7adf80928497f845fd8c2786cd53af25f8c9fe1bba24e3c3860162635bbed58f06c
f6c9966bb9b570987a48329279bb84afb9e464bb4ad19ae6600175086e28929569027c5285d2ed97615e5a7dada40ba
03c440861f524475":0

AES-GCM
NIST Validation (AES-256,128,1024,0,64) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"a0b1a62e46e7712277fc711e19d0c0c865ee77b42ac964b
7202dbcaf428086c2":"7dd7c0787fdbea4aacf929341659dcf4b75cbca8f92001e8b62a4d7b40272c5755fa9c445857db
05328dc11ce5221f044f4b3dafbf0e2d72a1ad0d3e4c804148db578218690ccc620d8b97b4450ff83400a6caaa9596176
11446a6627138a4067be9ea410d4b0581022ab621928205b4a4480560fc4c2c3b39a2805684006f35":"e20957a49a27
e247d00379850f934d6c":"":64:"c99751516620bf89":"9307620479f076c39f53965c87d20c2aff11c736c040dba74cd
690d275591a5defc57a02f6806de82eb7051548589484364f6c9b91f233a87258ede1ee276cb2c93b4fc76f4d7e60cbd2
9ba2c54cb479c178fa462c1c2fb6eeb3f1df0edfb894c9222b994c4931dedf7c6e8ddecbde385ddf4481807f52322a47bf
5ff7272991":0

AES-GCM
NIST Validation (AES-256,128,1024,0,64) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"ffcc1c88fba1723b3ab57b458d9bffb98b878c967fb43b9d
b2ae0753d32a3bb1":"19b6dec86d93c466307de3a36c0791ed1010b1b9cf8d30347ae46e0f9283c9fda43da8cb491dd1
7cc4298b1f0b876d6a0f4bcbc9667fe34564bc08f8f7b67045057d19f4bf027bc839e590822fa09a5cef1af18e64a0116a
a2a01a3f246c2b5272c18c9aa23efe674ba53d533ae8f0695cb78c1155cdc7a9d7fae2c4567dc07c":"d533c2170c5dc20
3512c81c34eff4077":"":64:"167ec8675e7f9e12":"0539287ac546fe5342e4c3c0ec07127dcd22899abfe8cdd6e89d08f

1374d76e877bec4844d06e0a9f32d181c8d945ba16a54ce3725fae21d8245c070a4da0c646203d6b91325b665ab98c30
295851c59265b4ab567b968b6e98536b7850738d92e9627b4c9c6f5d9ae2520944783d8f788a1aa11f3f5245660d41f3
88e26e0a1":0

AES-GCM NIST Validation (AES-256,128,1024,0,64) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"55e94b339c3bafe068ef9cc30787cc67058501149768437
77c92b4b331801650":"147cc7bc4008dadf1956520b5998d961499bdf3d8b168591adbfd99411ad7b34eb4b2a5c1bb0
522b810fec12dd7c775784d7ecdc741e6dec8191361e6abf473b219221801951b4d5ffe955ab50eef9cffdfee65ba29ddf
a943fb52d722825338c307870a48a35f51db340aa946c71904d03174b1e4a498238b9d631a6982c68d":"2e2b31214d6
1276a54daf2ccb98baa36":"":64:"5266e9c67c252164":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,1024,0,32) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"13c9572bdef62510d84f2d415cc481cd1e71b9c1132b43e
63b21ba4e16de9b39":"7c78e634dec811173ff3c4a9a48ae3ae794fbd2aefd4b31701777ff6fcb670744c592a1d298d31
9717870dca364b2a3562a4ffa422bf7173c4f7ea9b0edf675e948f8370ffd0fd0d5703a9d33e8f9f375b8b641a1b1eecd16
92ad1d461a68d97f91f9087f213aff23db1246ee16f403969c238f99eed894658277da23ced11ee":"a8339ba505a14786
ad05edfe8cebb8d0":"":32:"df3cab08":"91f9780daefd2c1010c458054ac6e35baa885cdd2c95e28e13f84451064e31e0
739f27bf259cb376ab951e1c7048e1252f0849ccb5453fc97b319666ebbfbc7ef3055212a61582d1b69158f3b1629950a
41bc756bded20498492ebc49a1535d1bd915e59c49b87ffebea2f4ad4516ecdd63fa5afda9cce9dc730d6ab2757384a":0

AES-GCM
NIST Validation (AES-256,128,1024,0,32) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"30a14ca53913acbb215b4e4159083106db3fff83cbedd1e5
425f65af1e94f5dd":"8c5f73ee1544553b712ad7a14f31379c8d54a4e432fb6c5112436988d83c4e94954b0249b47053
8fb977b756fbee70b811d4dc047a869e207bb0b495f1e271d0034e912000e97594033e0dedde0591b297f8a84bafcc93a
46268a5bba117b558f1c73513e971c80a7083e1718fc12d0cc0d996a8e09603d564f0b8e81eea28bc":"4f23f04904de76
d6decd4bd380ff56b1":"":32:"18e92b96":"bb4b3f8061edd6fa418dd71fe22eb0528547050b3bfbaa1c74e82148470d5
57499ce856de3e988384c0a73671bf370e560d8fda96dabe4728b5f72a6f9efd5023b07a96a631cafdf2c878b2567104c
466f82b89f429915cf3331845febcff008558f836b4c12d53e94d363eae43a50fc6cb36f4ca183be92ca5f299704e2c8cf":
0

AES-GCM NIST Validation (AES-256,128,1024,0,32)
#2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"e69f419140289ac25fb0e2ef9cc4f7e06777ac20f7d631918
d1af0c8883b7d6a":"ff8dfa4e70490ea9c84cb894dc5d7e1b935ebcdea80a39c4161d4db42cbb269cc86abd381af15ec9
a4a42ed18c1eed540decec19722df46f22aa06883297cb393fb23e4bb31a817e88357aa923c7ecbcf24c28a09f622dd21f
a70c0a02193024fdcefeaa96cc1b50f81a65dfa9e1bb5126f0c9766a861eed096ec15fb07b0f81":"531248afdaaf1b86cf3
4d2394900afd9":"":32:"c6885cdd":"f75299e0ead3834fc7ebd4b2051541b598ad57cc908fdcd4324cf4ccf7dcf7b3f07
37ad6c026399a8b1b6d3d50011b3c48ea2c89833b4b44c437677f230b75d36848781d4af14546894eecd873a2b1c3d2f
cdd676b10bd55112038c0fdaa7b5598fe4db273a1b6744cba47189b7e2a973651bfc2aaa9e9abea4494047b957a80":0

AES-GCM NIST Validation (AES-256,128,1024,1024,128) #0
depends_on:MBEDTLS_AES_C

gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"404a5d1ac9e32f9caabffbfa485ce9c27edc9e5cde0f2aab4f32ce3121449b88":"b63ec4d28854b7fe2d4d13973f5bcb16f78494ce25cc2820de9d0dc1d8d91db1f19bc9e01cee8418c9e88a69b2f30cdbb0dbdbb50be71e1e666c111c126f2b7197c02f69a1b2ec5e1bf4062b2d0b22fb0fa1585b4e6286b29f6ac98d1b1319dd99851fa6921607077d2947140fdeeea145b56ea7b6af276c9f65393bc43ede33":"b6e6c078e6869df156faa9ac32f057c3":"6ebc75fc9304f2b139abc7d3f68b253228009c503a08b7be77852da9e1afbe72c9ab374740b0dc391fa4d7e17de6a0aa08c69e6f5c5f05411e71e70c69dfbcf693df84c30f7a8e6c7949ea1e734297c0ea3df9b7e905faa6bbdcaf1ff2625a39363308331d74892cf531cb3f6d7db31bbe9a039fca87100367747024f68c5b77":128:"94c1b9b70f9c48e7efd40ecab320c2d3":"56a0ac94f3ec7be2608154f779c434ee96db5ed4f5a6e1acfb32361ce04e16e1337be5978df06d7c4f6012385fb9d45bb397dc00f165883714b4a5b2f72f69c018ffa6d4420ad1b772e94575f035ad203be3d34b5b789a99389f295b43f004de3daaef7fa918712d3a23ca44329595e08da190e3678bc6ad9b500b9f885abe23":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,128) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"b56f0c980acf7875cf7f27d53ad4a276adc126d0b93a5774ac4277eecad4309e":"2c94299e36b7c4a825ecbc5a7809061e0a6761764a5a655ffdb0c20e5c3fcb10f4e93c68aa0a38c2acc5d06f2b7c4ff4fcf814b551bfefa248dbe06a09a0f153213538a31fa7cf7d646b5b53908d8978f514c9c4d6d66f2b3738024b5f9c3fd86b6da0c818203183f4205f186ea44a54edb911b1a17c424c95852c8d271b2e93":"b004c049decfb43d6f3ec13c56f839ef":"b2045b97fbb52a5fc6ff03d74e59dd696f3f442c0b555add8e6d111f835df420f45e970c4b32a84f0c45ba3710b5cd574001862b073efa5c9c4bd50127b2ce72d2c736c5e2723956da5a0acb82041a609386d07b50551c1d1fa4678886bac54b0bd080cc5ef607dca2a0d6a1e71f0e3833678bf8560bc059dae370ec94d43af6":128:"fce7234f7f76b5d502fd2b96fc9b1ce7":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,128) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"1c5027c36e6caa1b3e5e45fead32b5e3126ac41f106c491b0b3a7c16502f4fe6":"58f0ceaa31c0025d2e6bb58720cce4b64f5f6c657c847ae42936eb1e343fea397c8a8cf2f5ef02ffaec25f431900dcb0910cf32cea9eca3b78aed1c451c7af51066489f87b2a5f8cf28d6fdb6ce49d898b6167b590a3907be7618be11fb0922a3cfd18e73efef19e5cdc250fa33f61e3940c6482ae35f339e8c0a85a17379a4e":"3ee660f03858669e557e3effdd7df6bd":"93e803c79de6ad652def62cf3cd34f9addc9dd1774967a0f69e1d28361eb2cacc177c63c07657389ce23bbe65d73e0460946d31be495424655c7724eac044cafafe1540fcbd4218921367054e43e3d21e0fa6a0da9f8b20c5cdbd019c944a2d2ee6aa6760ee1131e58fec9da30790f5a873e792098a82ddf18c3813611d9242a":128:"ac33f5ffca9df4efc09271ff7a4f58e2":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,120) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"34c3019810d72b5e584f0758f2f5888a42729a33610aafa9824badade4136bbd":"22deef66cbb7db240c399b6c83407f090d6999ba25e560b2087fed0467904bb5c40cbaa05b8bf0ff5a77c53fa229478d8e0736414daf9c420417c391c9a523fd85954533f1304d81359bdcc2c4ac90d9f5f8a67a517d7f05ba0409b718159baf11cd9154e815d5745179beb59954a45a8676a375d5af7fae4d0da05c4ea91a13":"f315ea36c17fc57dab3a2737d687cd4f":"f33c5a3a9e546ad5b35e4febf2ae557ca767b55d93bb3c1cf62d862d112dbd26f8fe2a3f54d347c1bc30029e55118bab2662b99b984b8b8e2d76831f94e48587de2709e32f16c26695f07e654b703eba6428f30070e23ed40b61d04dd1430e33c629117d945d9c0e4d36c79a8b8ab555d85083a898e7e7fbeb64a45cc3511d99":120:"0bae9403888efb4d8ec97df604cd5d":"FAIL":0

AES-GCM

NIST Validation (AES-256,128,1024,1024,120) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"29397d98fc5a7f04b5c8b6aa3a1dd975b6e4678457ae7f06
91eee40b5397503a":"0bbf1079cb5569c32257bc7e52371db46f3961b457402b816588243b4523543430d5ca56b52de
6632724c51e6c3af310b28822c749a12bdd58dee58bbc3266631562a998ec3acdc8a2567a9f07f7f9759c3f50b1d1dcdd
529256b80c0d227fc1fe8b58c62d1c643f1ac2996809fd061afcf4a9af184c14db9e63ec885c49de61":"885543a45fd116
3e34ef9276145b0f8c":"d88beaa0664bcef178cbdbfab17ff526b5c0f8ad9543c6a312d93c336707fbf87c0448b07a5505
80953279f552f368225cc6971f1eecc718d6aad1729c8d8873081357752bd09d77075fa680cb2dc4139171e4a0aaa50b
28c262c14fd10b8d799ca1c6641bb7dfdfdf3dea69aa2b9e4e4726dc18b0784afa4228e5ccb1eb2422":120:"7b334d7af
54b916821f6136e977a1f":"FAIL":0

AES-GCM NIST Validation (AES-256,128,1024,1024,120)
#2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"7555dfcf354da07fd70f951d94ec1d86a635edfdb7929460
207b2a39cc0cf4a3":"a1351cfffd1b0cbf80c3318cc432d3238cb647e996b7b53c527783594683f535950cd08788687c7
7226b2d3f095955884adc2e475ca1e1eab04e37d5e901ae8934a9d3a0cb37b80612ca25d989856dfa7607b03039b64d7
dcd468204f03e0f2c55cb41c5367c56ca6c561425992b40e2d4f380b3d8419f681e88ebe2d4bdad36":"e1b30b6a47e8c
21228e41a21b1a004f0":"bf986d3842378440f8924bb7f117d1a86888a666915a93ba65d486d14c580501e736d3418c
ebee572439318b21b6e4e504a7b075b8c2300c014e87e04fa842b6a2a3ebd9e6134b9ddd78e0a696223b1dc775f3288a
6a9569c64b4d8fc5e04f2047c70115f692d2c2cefe7488de42ff862d7c0f542e58d69f0f8c9bf67ef48aea":120:"d8ef543
8b7cf5dc11209a635ce1095":"95e8db7c8ecab8a60ceb49726153a7c5553cf571bc40515944d833485e19bf33cb954e2
555943778040165a6cfffecef79eb7d82fef5a2f136f004bb5e7c35ae827fac3da292a185b5b8fc262012c05caeda5453ed
e3303cfeb0c890db1facadaa2895bdbb33265ada0bb46030607b6cf94f86961178e2e2deeb53c63900f1ec":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,112) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"bbeafe86c72ab0354b733b69b09e4d3462feb1658fe40400
4d81503f3a6e132f":"a033c2051e425d01d97d563572e42c5113860e5dedcd24c76e3e357559ba3250f1fc5d4a931a9d
0900ac025400f0158621f0b1215b2907467bfc874bcabbb28e28de81fe1ee5b79985261c512afec2327c8c5957df90c9e
b77950de4a4860b57a9e6e145ea15eb52da63f217f94a5c8e5fcb5d361b86e0e67637a450cdbcb06f":"ee1caba93cb549
054ca29715a536393e":"e44b0e0d275ae7c38a7dc2f768e899c1c11a4c4cb5b5bd25cd2132e3ecbaa5a63654312603e1
c5b393c0ce6253c55986ee45bb1daac78a26749d88928f9b9908690fc148a656b78e3595319432763efbcf6957c9b215
0ccabfd4833d0dcee01758c5efb47321a948b379a2ec0abcd6b6cbf41a8883f0f5d5bf7b240cb35f0777":112:"a4809e07
2f93deb7b77c52427095":"e62adf9bbd92dd03cc5250251691f724c6ece1cb89d8c4daf31cc732a5420f6bedab71aab02
38ba23bd7165ed1f692561ef457fd1d47413949405b6fc8e17922b17026d89d5830b383546ea516a56f3a1c45ec12515
83ae880fa8985bd3dcc1d6a57b746971937bf370e76482238cc08c2c3b13258151e0a6475cc017f8a3d0e":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,112) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"6ad06c88dd4f3becf35eed95bb859be2406a1803a66e4332
a74c5f75c09b9a01":"2219c11672884b93d0290b6a7140feafe416461f1cdaf0b3aa64693d7db2eb10feae46aac7af549f
a1b0abc78c11f8df7ee803ef70310fc3e67769f8b4bc64f81143a6ebf8bee9d386a8ede5d2cc0ed17985a3b7bb95191ef5
5e684690ccdc5ca504bc6eb28442b353861a034a43532c025f666e80be967a6b05b9dd3a91ff58":"07d8b4a6e77aef90
18828b61e0fdf2a4":"cca1fd0278045dda80b847f0975b6cbf31e1910d2c99b4eb78c360d89133a1c52e66c5c3801824
afc1f079d2b2b1c827199e83f680e59b9a7de9b15fa7b6848b5bf4e16a12ac1af4cf2b4d7bb45673c5e1241e999644086

0a9204fc27cae46a991607bc5e7120d6c115ddcbdd02c022b262602139081e61eee4aba7193f13992":112:"e3ede1703
86e76321a575c095966":"FAIL":0

AES-GCM NIST Validation (AES-256,128,1024,1024,112) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"87bbf7c15689e8c99a5a32a8ba0dfebcfe1989159807428c
dd1f382c3ea95178":"b77d3bf3b30b3e6e5c86cbfb7e5455f6480f423cc76834b4663d28d9f1eb5c40212634e3347668
427f7848352ab789886f96682a568260bdaeb7de0aae2af36f5ae04f06c332b158d923706c1c6255c673feeadb6d30bfc9
01e60b92acd9ddd83ef98686c4d492f4a60e97af2541d470a6a6b21903441020ea7619cf28a06986":"2f19aa1f3a82a73
98706953f01739da7":"590dbd230854aa2b5ac19fc3dc9453e5bb9637e47d97b92486a599bdafdfb27c3852e3d06a914
29bb820eb12a5318ed8861ffe87d659c462ef167be22604facfa3afb601b2167989b9e3b2e5b59e7d07fda27ffccd45086
9d528410b0aff468f70cc10ef6723a74af6eebc1572c123a9b5a9aab748a31fa764716d3293ff5de7":112:"5c43fc4dc959
fabeebb188dbf3a5":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,104) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"24095a66b6eb0320ca75e2ab78e8496a45f4b000fc43436
904c3e386fb852ed2":"4690edc843e23d9d9b9a4dab8fa8193f8bf03897d3d29759e9dc9e0f8a970c0f5d4399b9f60461
fe5cf439f9b0d54bbc075695e4d76b76298cc2b75bb3e0b516ee9ada93f77c4c002ba9fd163a1e4b377befb76c1e5ab8b
3901f214c0a4c48bd2aa2f33560d46e2721a060d4671dc97633ff9bcd703bb0fbed9a4a2c259b53f3":"0955c1f0e271ed
ca279e016074886f60":"f5160c75c449e6bb971e73b7d04ab9b9a85879f6eb2d67354af94a4f0ca339c0a03a5b9ede87a
4ff6823b698113a38ae5327e6878c3ccc0e36d74fe07aa51c027c3b334812862bc660178f5d0f3e764c0b828a5e3f2e7d
7a1185b7e79828304a7ad3ddcd724305484177e66f4f81e66afdc5bbee0ec174bff5eb3719482bd2d8":104:"75a313475
98f09fceeea6736fe":"0dd2dca260325967267667ff3ccdc6d6b35648821a42090abba46282869bac4bdc20a8bee024be
a18a07396c38dbb45d9481fedcc423a3928cfa78a2f0ae8eedb062add810bdbee77ddc26c29e4f9fda1ab336d04ef42947
b05fbdb9bc4df79e37af951d19d6bf5e5cb34eef898f23642a9c4a9111ed0b7a08abeeefbbd45c23":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,104) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"086b77b5731f971f0bf5b8227361b216746daf8b08c583a
d38f114a64aa7877b":"629317212ff8bd8a7676e4c00b81a9577de6397c832f99ac974fa2bbbccb6e3b8aa776db6922ee
d0b014bf3923799da7d9d0854c8817470e1e2f7fc7a572f9d0316ee60cde7ef025d59b897d29a6fee721aeb2f7bb44f9af
b471e8a7b0b43a39b5497a3b4d6beb4b511f0cefa12ce5e6d843609d3e06999acfbee50a22ca1eee":"164058e5e425f9d
a40d22c9098a16204":"6633eae08a1df85f2d36e162f2d7ddd92b0c56b7477f3c6cdb9919d0e4b1e54ea7635c202dcf5
2d1c688afbbb15552adda32b4cd30aa462b367f02ded02e0d64eeee2a6b95462b191784143c25607fd08a23a2fbc75cf6
bee294daf2042587fdd8fe3d22c3a242c624cf0a51a7c14db4f0f766ec437de4c83b64f23706a24437":104:"2eb6eb6d51
6ed4cf1778b4e378":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,104) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"0f9e806b0d937268561c0eafbbdd14ec715b7e9cef4118d6
eb28abbb91266745":"2ae4baef22ace26f464a9b0c75802303f2d7c0f9a1ed1d0180135189765bdd347fea0cc2b73ee7f
bbf95ea1fda22597b8aad826f63e744069a9c349488b2cc1cf9372f423cc6503020821257247 30ae5a4d878e07385ddc9
9034c6b6b46748f02c80b179fe6406b1d33581950cb9bcd1d1ea1ec7b5becfd6c1f5b279412c433a":"8657996634e74d
4689f292645f103a2e":"2ca253355e893e58cb1a900fbb62d61595de5c4186dc8a9129da3657a92b4a631bbdc3d5f863

95385a9aa8557b67f886e3bb807620e558c93aea8e65826eadeb21544418ee40f5420c2d2b8270491be6fc2dcbfd12847fa350910dd615e9a1881bc2ced3b0ac3bde445b735e43c0c84f9d120ca5edd655779fc13c6f88b484f7":104:"83155ebb1a42112dd1c474f37b":"87d69fc3cbc757b2b57b180c6ba34db4e20dde19976bfb3d274d32e7cea13f0c7d9e840d59ce857718c985763b7639e448516ddbbda559457cd8cb364fa99addd5ba44ef45c11060d9be82b4ebe1f0711ac95433074649b6c08eeab539fdfc99c77498b420427e4d70e316111845793de1f67fb0d04e3389a8862f46f4582dc8":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,96) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"c24c17911f6db4b3e37c46bcc6fa35efc1a55f7754f0bb99f2eea93398116447":"0bd92cb106867e25ad427ff6e5f384d2d0f432fc389852187fcc7b0bf9f6d11a102a872b99ed1ad9a05dab0f79fa634745535efed804ff42b0af8dad20ba44709391fb263f245e5a2c52d9ce904179633282f57a1229b0a9c4557a5c0aeda29bbc5a7a871fa8b62d58100c3722c21e51e3b3e913185235526e7a5a91c559717d":"5098cc52a69ee044197e2c000c2d4ab8":"9ad4dee311d854925fc7f10eca4f5dd4e6990cb2d4325da2ef25a9a23690f5c5590be285d33aaeba76506c59edec64b8c3ff8e62716d1c385fbce2a42bc7bd5d8e8584de1944543ab6f340c20911f8b7b3be1a1db18a4bb94119333339de95815cae09365b016edc184e11f3c5b851f1fa92b1b63cfa3872a127109c1294b677":96:"f7930e3fab74a91cb6543e72":"6124ede608d416baa5e653a898ca76e9f47f08403c1984feec112e670ded2226e0073f8881ab2161cfda541dccae19691285f7391a729f07aba18f340bb452c1da39cbe83cf476cfc105b64187e0d2227dd283dcba8b6a350f9956b18861fa131d3f00c034443e8f60e0fdfcfaabbed93381ae374a8bf66523d33646183e1379":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,96) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"d267a8379260036ff3d1ec07a7b086ff75706bad12d37d9656f04776f3d8b85c":"80c68a330ef50e3e516681f1e535868b03466e7edbb86cb385d01db487da3dd3edad940fdc98d918b7db9b59f8d61369eee2928c88557306c4a13e366af0708d94cb90a15f1c3bc45544bdb05ff964da5e06c5ae965f20adb504620aed7bce2e82f4e408d00219c15ef85fae1ff13fea53deb78afa5f2a50edbd622446e4a894":"674dc34e8c74c51fa42aacd625a1bd5b":"6a9a8af732ae96d0b5a9730ad792e296150d59770a20a3fdbbc2a3a035a88ac445d64f37d684e22003c214b771c1995719da72f3ed24a96618284dd414f0cac364640b23c680dc80492a435c8ec10add53b0d9e3374f1cf5bfc663e3528fa2f6209846421ea6f481b7ecf57714f7bc2527edc4e0466b13e750dd4d4c0cc0cdfc":96:"bea660e963b08fc657741bc8":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,96) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"c86cb637753010f639fa3aa3bff7c28b74f012ad6090f2a31b0801d086f183ad":"6b7858557e0fd0f957842fb30e8d54dedbc127eb4bbf9de319f731fa28a606df2c046a0bce8ecda4e75d3596e4e988efd6bc279aa005bc52fad92ba07f5b1dfda4cc417029f9778c88d6fe5341a0fd48893dcb7c68d0df310a060f2a5235aee422d380f7209bc0909b2aa7e876044056f0b915dab0bc13cbea5a3b86d40ca802":"87ff6e0bb313502fedf3d2696bff99b5":"2816f1132724f42e40deabab25e325b282f8c615a79e0c98c00d488ee562375372402349665 65e46bfb0c50f2b10366d1589620e6e78bd90ade24d38a272f3fff53c09466aa2d3ef793d7f814a064b713821850a6e6a058f5139a1088347a9fa0f54e38abd51ddfc7ef040bf41d188f3f86c973551ced019812c1fc668649621":96:"7859f047f32b51833333accf":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,64) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"2c31ca0cac3efe467168198f06beacf39565a6f57f82e1048

a5c06a231315882":"65261d6e29b2369b1828a7cef2df9873d6e6057c499301afedd6cb65b5036ddb95f9e353fbf38e5
4c4f46f88164325b33620ce183beb2e411fbb89a0e0002e542fc161cad32a61ee6f1e1717e0b4dcd0340b116f795bc100
9dbbc65bc31c9b549bf03c40bc204cd0d02ec884be907777ebeed8b527ec3af7cbb508193c0745de":"95cae6e85f33f30
43182460589be3639":"67523751a9b1b643d00de4511b55e4268cb2d18e79e01a55fc7b677d529bd6400940fb25ea6a
e135c1a816e61b69e90b966981aeda685934b107066e1467db78973492ad791e20aef430db3a047447141def8be6e6a9
a15089607c3af9368cdb11b7b5fbf90691505d0c33664766945d387904e7089b915a3c28886ba1763bb5":64:"21309d
0351cac45e":"1d5f2cb921f54aeb552b4304142facd49497837deb1f00d26fbeddbab922fd80b00dba782961f8fce84f1f
7973e81eed6ee168b1760c575c891f40a1dae0fa1a08738025d13ef6e0b30be4f054d874f1b8a2427a19ebb071d98365c
32316a88a68c2b40daf1ea831a64519ac3679acb4e04986ecc614ec673c498c6fee459e40":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,64) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"ca9fa36ca2159dff9723f6cfdb13280446eb6bc3688043c7e
2e2504184791596":"ac04c4293554cd832aa400c811cb202d815d6178aa1343b4628592b7f3ae45dc5f12ea47be4b43e
1865f40b06ab67b3a9fb3644248a9b3efe131a8addb7447978bb51ccf749e75574fea60e8781677200af023b2f8c415f4e
6d8c575a9e374916d9ec3a612b16e37beb589444b588e0b770d9f8e818ad83f83aa4ecf386d17a7":"d13ca73365e5711
4fc698ee60ba0ad84":"2aa510b7f1620bfce90080e0e25f5468dbc5314b50914e793b5278369c51ac017eace9fd15127f
ca5a726ad9e67bdee5af298988d9a57ec4bbc43d4eb849535eb10521ac7cd7ed647479a42876af2ebc9e2108b539febda
a9127c49bda1bda800f6034050b8576e944311dfbca59d64d259571b6d2ed5b2fc07127239b03f4b7":64:"2111d55d96
a4d84d":"FAIL":0

AES-GCM NIST Validation (AES-256,128,1024,1024,64) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"2f802e838250064c15fdee28d7bd4872850355870847701
ad9742b2d6eb4b0c0":"e2ca8c8d172ff90232879f510d1225af91bc323bdf636363c2903fcd1790692c8bcb03a1cccb18
814678852c6b3a441552e541b843ee5e4f86a152fa73d05aea659fe08aa6428bb257eaa2a7b579fdc4022c1dec359a854
253c1aefc983c5ede8c97517ea69fc4606e25f13ffb0f5f49160691454fbb74e704326738353525f7":"2dd550cfd97f8e1
d8d31ba5537ae4710":"72b9630dda40306e785b961934c56e20948f8eac0e981f49787eb3dbd6e4607f7d08d10ca6437
46bf1efa7e5066993683d527a90f2d45ec9cf73113f1f17bb67958be669acd4e2927f1dacfde902cd3048056d7f6dfdd86
30ff054efce4526db7c9321d6d2be2236f4d60e27b89d8ec94f65a06dc0953c8c4533a51b6a29bd2c":64:"bd6c8823c90
05c85":"f6dd0b5f3d1a393a1837112962dba175a13c2d1e525ef95734caf34949d8b2d63b4fe5603226b5f632f2d7f927
361ba639dc0e3c63414f45462342695916d5792133b4a24c7c4cbe2b97c712bf27ab62d3d68b3875d58ffe4b7c30a817
1bff1a9e2f3995768faacda2ea9213ff35798b9e4513f6a87bd3f5a9d93e847e768359":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,32) #0
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"84dd53ce0146cb71c32776033bb243098d78a22ac17f52a
62a122f5653fb4e33":"68222bffa782dcfe4f328fc20eb520e75a9a5fedbe13ec7fcf0e82fba08bb87a8a8e02902638e32f
e0e2294344b380797f8028426ffcc0531c739c884892394c48ff0779c5f5edf0a36a3fb8aa91213347774ec4bf0fe1049b
d53746b13beef3c637169826c367056cb1aa0a3868e23f886a9c7b8015c26af9e40794662f6b21":"f0c90a1bca52f30fa
b3670df0d3beab0":"a3ea8032f36a5ca3d7a1088fd08ac50ae6bdc06ad3a534b773ac3e3d4a3d524499e56274a0062c5
8c3b0685cc850f4725e5c221af8f51c6df2bbd5fbcff4a93ba4c1054f7f9c67fd9285511a08d328d76a642f067227d378f9
5a1e67587b90251f9103ed3cacdb6bf69e0794e366d8b92d8de37b4e028de0778841f356ac044d":32:"b1ece9fb":"FAI
L":0

AES-GCM

NIST Validation (AES-256,128,1024,1024,32) #1
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"9bb36fe25e966a075ae2c3bb43b5877679ebc379d5123c8eda3fa0e30b95cae0":"fb3a4be643c10343251c6f0745aaa54349463f622ca04a792e9b4780866844b30aeef3269fc60cac0ea031c5f3780b535e15154f7c76eb4a371b8ae368550f3fa2ce693c34511ec96b839cac567f1b0de0e7e3116d729b45d1b16e453703a43db73f5d0c3e430f16b142420b5f0d26d72ac3dba543d7d813603b0bfdca3dd63e":"59869df4ef5754b406478a2fb608ee99":"ecd125682e8a8e26757c888b0c8b95dec5e7ed7ac991768f93e8af5bcf6f21ed4d4d38699ee7984ed13635fff72f938150157c9a27fcda121ffced7b492d2b18dad299cb6495ed5f68441aefc8219d2cf717d15d5cd2dbce4606fcf90fe45f3601127cf6acee210bd7df97309f773974a35bef1d33df984101c2fc9d4b55259e":32:"cb3f5338":"FAIL":0

AES-GCM
NIST Validation (AES-256,128,1024,1024,32) #2
depends_on:MBEDTLS_AES_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_AES:"ca264e7caecad56ee31c8bf8dde9592f753a6299e76c60ac1e93cff3b3de8ce9":"8d03cf6fac31182ad3e6f32e4c823e3b421aef786d5651afafbf70ef14c00524ab814bc421b1d4181b4d3d82d6ae4e8032e43a6c4e0691184425b37320798f865c88b9b306466311d79e3e42076837474c37c9f6336ed777f05f70b0c7d72bd4348a4cd754d0f0c3e4587f9a18313ea2d2bace502a24ea417d3041b709a0471f":"4763a4e37b806a5f4510f69fd8c63571":"07daeba37a66ebe15f3d6451d1176f3a7107a302da6966680c425377e621fd71610d1fc9c95122da5bf85f83b24c4b783b1dcd6b508d41e22c09b5c43693d072869601fc7e3f5a51dbd3bc6508e8d095b9130fb6a7f2a043f3a432e7ce68b7de06c1379e6bab5a1a48823b76762051b4e707ddc3201eb36456e3862425cb011a":32:"3105dddb":"FAIL":0

AES-GCM
Bad IV (AES-256,128,0,0,32) #0
depends_on:MBEDTLS_AES_C
gcm_bad_parameters:MBEDTLS_CIPHER_ID_AES:MBEDTLS_GCM_DECRYPT:"ca264e7caecad56ee31c8bf8dde9592f753a6299e76c60ac1e93cff3b3de8ce9":"":"":"":32:MBEDTLS_ERR_GCM_BAD_INPUT

AES-GCM Selftest
depends_on:MBEDTLS_AES_C
gcm_selftest:
-----BEGIN CERTIFICATE-----
MIIDFTCCAf0CDFOittkjXbxFc/m3bDANBgkqhkiG9w0BAQsFADBOMRowGAYDVQQD
ExFzZXJ2ZXIxL2ludC1jYS12MTEQMA4GA1UECxMHdGVzdGluZzERMA8GA1UEChMI
UG9sYXJTU0wxCzAJBgNVBAYTAk5MMCIYDzIwMTQwNjE5MTAwOTI5WhgPMjAyNDA2
MTgxMDA5MjlaMEQxEDAOBgNVBAMTB3NlcnZlcjIxEDAOBgNVBAsTB3Rlc3Rpbmcx
ETAPBgNVBAoTCFBvbGFyU1NMMQswCQYDVQQGEwJOTDCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBAMFNo93nzR3RBNdJcriZrA545Do8Ss86ExbQWuTNowCI
p+4ea5anUrSQ7y1yej4kmvy2NKwk9XfgJmSMnLAofaHa6ozmyRyWvP7BBFKzNtSj
+uGxdtiQwWG0ZlI2oiZTqqt0Xgd9GYLbKtgfoNkNHC1JZvdbJXNG6AuKT2kMtQCQ
4dqCEGZ9rlQri2V5kaHiYcPNQEkI7mgM8YuG0ka/0LiqEQMef1aoGh5EGA8PhYva
i0Re4hjGYi/HZo36Xdh98yeJKQHFkA4/J/EwyEoO79bex8cna8cFPXrEAjyaHT4P
6DSYW8tzS1KW2BGiLICIaTla0w+w3lkvEcf36hIBMJcCAwEAATANBgkqhkiG9w0B
AQsFAAOCAQEAivCCMBfC5YNeozwp8vAWpiRUakhtO8ysvCfQsZD4tWLlSkrjoUtG
3RNd9gDVDGb852GswtNMKHJC1AeZuXdh3eBoDBNTXnR/9UkHgWNBy5f+JH2irYrc
ps5ofpYJZe7K6xQjl+RLc8nfUUaVfS3dJnyLr9k5kg4in48p+hEF6oXDBu2zdufF
53k/U98FTvFkVisEDFzLXyKX0fAZxfMk4qnEoBflH4fEXfkuuaBUVdoGGIMRLNAW

```
GIyRxr+zj+OJL+ZjjAkY4JqtEuUuLjODn//DHI/MkqE0LANOvbb4akpgZsyvSSO3
o38d1wQHw5+bO+YDqdfIdQXguU5mtS1xAw==
-----END
 CERTIFICATE-----
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
   <Configuration>Release</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\x509\cert_write.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">

   <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid>{35E52E46-3BA9-4361-41D3-53663C2E9B8A}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>cert_write</RootNamespace>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
```

```
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
/>
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
```

```
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
   <PrecompiledHeader>
   </PrecompiledHeader>
   <WarningLevel>Level3</WarningLevel>
   <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
    <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
   <SubSystem>Console</SubSystem>
   <GenerateDebugInformation>true</GenerateDebugInformation>
   <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
   <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
   <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
   <PrecompiledHeader>
   </PrecompiledHeader>
   <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
 <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
   <SubSystem>Console</SubSystem>
   <GenerateDebugInformation>true</GenerateDebugInformation>
   <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
   <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
   <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
```

```
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
  </Link>
 </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
 <Import
 Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
```

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 11 (0xb)
    Signature Algorithm: sha512WithRSAEncryption
    Issuer: C=NL, O=PolarSSL, CN=PolarSSL Test CA
    Validity
      Not Before: Feb 12 14:44:07 2011 GMT
      Not After : Feb 12 14:44:07 2021 GMT
    Subject: C=NL, O=PolarSSL, CN=PolarSSL Cert SHA512
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (2048 bit)
        Modulus (2048 bit):
          00:b9:3c:4a:c5:c8:a3:8e:90:17:a4:9e:52:aa:71:
          75:26:61:80:e7:c7:b5:6d:8c:ff:aa:b6:41:26:b7:
          be:11:ad:5c:73:16:0c:64:11:48:04:ff:d6:e1:3b:
          05:db:89:bb:b3:97:09:d5:1c:14:dd:68:87:39:b0:
          3d:71:cb:e2:76:d0:1a:d8:18:2d:80:1b:54:f6:e5:
          44:9a:f1:cb:af:61:2e:df:49:0d:9d:09:b7:ed:b1:
          fd:3c:fd:3c:fa:24:cf:5d:bf:7c:e4:53:e7:25:b5:
          ea:44:22:e9:26:d3:ea:20:94:9e:e6:61:67:ba:2e:
           07:67:0b:03:2f:a2:09:ed:f0:33:8f:0b:ce:10:ef:
          67:a4:c6:08:da:c1:ed:c2:3f:d7:4a:dd:15:3d:f9:
          5e:1c:81:60:46:3e:b5:b3:3d:2f:a6:de:47:1c:bc:
          92:ae:eb:df:27:6b:16:56:b7:dc:ec:d1:55:57:a5:
          6e:ec:75:25:f5:b7:7b:df:ab:d2:3a:5a:91:98:7d:
          97:17:0b:13:0a:a7:6b:4a:8b:c1:47:30:fb:3a:f8:
          41:04:d5:c1:df:b8:1d:bf:7b:01:a5:65:a2:e0:1e:
          36:b7:a6:5c:cc:30:5a:f8:cd:6f:cd:f1:19:62:25:
          ca:01:e3:35:7f:fa:20:f5:dc:fd:69:b2:6a:00:7d:
          17:f7
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints:
        CA:FALSE
      X509v3 Subject Key Identifier:
        7D:E4:9C:6B:E6:F9:71:7D:46:D2:12:3D:AD:6B:1D:FD:C2:AA:78:4C
      X509v3 Authority Key Identifier:
        keyid:B4:5A:E4:A5:B3:DE:D2:52:F6:B9:D5:A6:95:0F:EB:3E:BC:C7:FD:FF

  Signature Algorithm: sha512WithRSAEncryption
    84:68:78:72:54:00:bf:8a:45:28:35:be:18:47:d8:69:f6:67:
    de:a6:f8:a6:d0:fd:9f:79:f7:e8:02:8a:c3:83:5d:85:45:cc:
    b6:98:77:a7:18:3f:6b:d2:e4:d0:af:d5:52:d9:db:7e:4a:d3:
    68:b0:08:64:14:de:c2:3b:1d:7b:ac:79:ad:49:5a:4c:f6:d2:
    35:ef:a4:8c:b7:5b:d1:0b:7b:50:c6:9c:48:3e:96:3b:1b:0b:
    0e:e8:10:3f:8c:3b:4f:6b:1d:5c:3a:27:f3:43:22:ac:37:11:
```

71:b8:07:66:b0:f8:71:c3:22:cf:f4:96:83:93:fb:42:b0:1a:
43:f9:4b:df:cb:5f:0f:ba:9e:80:f1:ff:08:3a:46:51:dc:d0:
36:bd:b1:c4:ca:fb:00:12:e7:e0:37:70:40:0e:73:19:63:c2:
e5:da:56:77:07:68:a5:40:9e:d6:0f:ad:b5:b3:b2:f5:3f:01:
e8:68:e7:a3:b0:d7:f3:dd:ff:b6:d7:8f:75:4e:25:ab:12:32:
99:45:ad:57:40:de:d7:b4:0d:d0:c3:66:89:47:f2:0c:b2:b5:
df:52:0e:fa:63:62:65:89:07:4a:80:69:0e:4e:ba:c0:43:5d:
05:75:22:cf:50:f9:ac:bd:ef:8d:8c:10:08:b6:8b:62:4f:a1:
60:55:a3:0d

-----BEGIN
CERTIFICATE-----

MIIDQjCCAiqgAwIBAgIBCzANBgkqhkiG9w0BAQ0FADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTEwMjEyMTQ0NDA3WhcNMjEwMjEyMTQ0NDA3WjA/MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxHTAbBgNVBAMTFFBvbGFyU1NMIENlcnQgU0hBNTEyMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuTxKxcijjpAXpJ5SqnF1JmGA
58e1bYz/qrZBJre+Ea1ccxYMZBFIBP/W4TsF24m7s5cJ1RwU3WiHObA9ccvidtAa
2BgtgBtU9uVEmvHLr2Eu30kNnQm37bH9PP08+iTPXb985FPnJbXqRCLpJtPqIJSe
5mFnui4HZwsDL6IJ7fAzjwvOEO9npMYI2sHtwj/XSt0VPfleHIFgRj61sz0vpt5H
HLySruvfJ2sWVrfc7NFVV6Vu7HUl9bd736vSOlqRmH2XFwsTCqdrSovBRzD7OvhB
BNXB37gdv3sBpWWi4B42t6ZczDBa+M1vzfEZYiXKAeM1f/og9dz9abJqAH0X9wID
AQABo00wSzAJBgNVHRMEAjAAMB0GA1UdDgQWBBR95Jxr5vlxfUbSEj2tax39wqp4
TDAfBgNVHSMEGDAWgBS0WuSls97SUva51aaVD+s+vMf9/zANBgkqhkiG9w0BAQ0F
AAOCAQEAhGh4clQAv4pFKDW+GEfYafZn3qb4ptD9n3n36AKKw4NdhUXMtph3pxg/
a9Lk0K/VUtnbfkrTaLAIZBTewjsde6x5rUlaTPbSNe+kjLdb0Qt7UMacSD6WOxsL
DugQP4w7T2sdXDon80MirDcRcbgHZrD4ccMiz/SWg5P7QrAaQ/lL38tfD7qegPH/
CDpGUdzQNr2xxMr7ABLn4DdwQA5zGWPC5dpWdwdopUCe1g+ttbOy9T8B6Gjno7DX
893/ttePdU4lqxIymUWtV0De17QN0MNmiUfyDLK131IO+mNiZYkHSoBpDk66wENd
BXUiz1D5rL3vjYwQCLaLYk+hYFWjDQ==

-----END
CERTIFICATE-----

-----BEGIN PRIVATE KEY-----

MG8CAQAwEwYHKoZIzj0CAQYIKoZIzj0DAQEEVTBTAgEBBBgzjoaogeI49Um9bwVT
SUtz49YRMP3GyW2hNAMyAARRdbzfMKNw851Tk+YScojYAWe19LS3dsZ098bzVLfS
JAYsH2hUtaevD+V46vJY8Cc=

-----END PRIVATE KEY-----

-----BEGIN CERTIFICATE-----

MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDYwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDcwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASNOj4d4MEA
7p/3miijqG4ToE4opKPAm+3BTIGrJTYT14++TSiUICl0ASXj+xeUcLMIaXTN042s
LsHxpShzQaL0o4GJMIGGMB0GA1UdDgQWBBREq5J3toJPxZ3O+ssJ5vkkU0RJEzBX
BgNVHSMEUDBOgBSjovYaC/m6Li9Tp0V9iZRs9267Q6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA1ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAKGcf+c442c/XiwubbaiQvsoZ7EoVxuM
oKmia0gPyBNkAiEA83asjJ5FDXQuLyZpczviXrbmqgCPOfYadtvkc0cxMis=

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDUwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDYwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASA9qWoAUHr
nn+3kxyNrjPJk82WDLimW21RN51uxpobadv8YgGEDRdP+Ok+uRqQSUsA6ZXfF3iG
r2GjfQ3wMDH8o4GJMIGGMB0GA1UdDgQWBBSjovYaC/m6Li9Tp0V9iZRs9267QzBX
BgNVHSMEUDBOgBTXh06MAV9S4l4lG1TKOrKRBh4qn6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA0ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgcjZNFWJtlDmoPZbAxqsGczRYK0lfPgu6
g1H7pp0ce+wCIDj9BRZM2OB9EF0e+MDKGjyZGfvfrL6Ir47x/KrM6H8T
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDQwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDUwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQEdT0OFf5G
UcrgX2XllCyJzP94NZ464GsgB6psNLsDeL+j7AU+oJy7VLvW/lHh3ODgl08Z9bhq
LFBmNjnHbm8Qo4GJMIGGMB0GA1UdDgQWBBTXh06MAV9S4l4lG1TKOrKRBh4qnzBX
BgNVHSMEUDBOgBQox4F1NsZunlsduoGvzIgRSYfB36EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAzggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAIW++zqDZlLLUk/emePohdNOp5JO3wS9
XvkBJ6Wua7GBAiAdx+EKmdjVrwnzrQltTgnmSfGMXhKNYifK3uD83W3pcQ==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDMwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDQwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQUXDgcUVNT
9hovbZE5HL6rjOb7C55wEuWKThV/CcZ4rWrXx7VXHYdD/R3aDA7JSvYpm2sTok4i
sblDzhZM/GDNo4GJMIGGMB0GA1UdDgQWBBQox4F1NsZunlsduoGvzIgRSYfB3zBX
BgNVHSMEUDBOgBQApzZdtBdD3dLxouQpr/aDiVttd6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAyggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgAkiNhqFAZXSUWEDK91OZvQGdeZOtd6mC
+Wv3fGk3t28CIEKOwidkUTUaiPdZ4efmAr+CEeGzdq27ob2S+nqqHqgV
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDIwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDMwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQRDXDNIi1p
ereudhqwa2LslXgsxnB63Hu5y5lg+1WPruIYPzD/Ho0APveVdzFLVji19+bE4+tF
PYL1SpsN1WfWo4GJMIGGMB0GA1UdDgQWBBQApzZdtBdD3dLxouQpr/aDiVttdzBX
BgNVHSMEUDBOgBT5RCgQ0AlZTQbfFB2+6+w0XRvydaEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAxggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAOnd+7bAofkHVa4KFNjv3TCegw1lrhuM

8Of8wgvrTEGoAiEAsS8iKMpSfXH4D0egg4gLamE6akde965rDtySU+ve9lg=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDEwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDIwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQWHpv1i6lf
wvNPOP5ka6S0n55EvzoaYK6pbTXP6yMOW/4XZSPKx5Zoq4FMe0cKzGIIFL1rzj1V
2czYB+qvLhyio4GJMIGGMB0GA1UdDgQWBBT5RCgQ0AlZTQbfFB2+6+w0XRvydTBX
BgNVHSMEUDBOgBSh3uHkX5nj86yFEFwjscSWM40P+qEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAI7unGW/gr9tOc3i+dF5N815srgh+FrX
oj9Et74EcSpTAiBubv+vOH0DE0gmYI11HeAIgutWqqMIC72dZlwTF/Vi3g==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB3jCCAYWgAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDAwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQznn9zHHwL
GO8VR4W9V7vMlxCdoojzEOiX5Y6JtPtFOz866ueHY6zoN0/mJ6DnqnSXilJIUUeW
6eGfqmka7nxko4GRMIGOMB0GA1UdDgQWBBSh3uHkX5nj86yFEFwjscSWM40P+jBf
BgNVHSMEWDBWgBQlFYvU5WboI4fcdPoiQs8/fPHZraEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggkA/KCWhcqToHAw
DAYDVR0TBAUwAwEB/zAKBggqhkjOPQQDAgNHADBEAiBasbuinP+pJTU4oDCVD8zQ
1rJBDSOKIEyWu84/D6Hj6wIgVMPUoO01bPhzllAa/gW8Xk/daey09SBgN3AT9pWU
TDA=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIBpTCCAUugAwIBAgIJAPygloXKk6BwMAoGCCqGSM49BAMCMC8xCzAJBgNVBAYT
AlVLMREwDwYDVQQKDAhtYmVkIFRMUzENMAsGA1UEAwwEQ0EwMDAeFw0xNzA2MjIx
MTUwMzJaFw0yNzA2MjMxMTUwMzJaMC8xCzAJBgNVBAYTAlVLMREwDwYDVQQKDAht
YmVkIFRMUzENMAsGA1UEAwwEQ0EwMDBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IA
BFW41/qAwAPpy+Txdc7PKmzZsq9CPiujKU4vpF1ekXnGx2HP420QobwBVVWhkzRm
LwdboH2j65dcCKjQ7mv/dxKjUDBOMB0GA1UdDgQWBBQlFYvU5WboI4fcdPoiQs8/
fPHZrTAfBgNVHSMEGDAWgBQlFYvU5WboI4fcdPoiQs8/fPHZrTAMBgNVHRMEBTAD
AQH/MAoGCCqGSM49BAMCA0gAMEUCIQC7iRcVzwMyfVK5imirJ7MqJQ04euH4CLOt
IZ+SNfaERAIgSU0MWFDosVEIpg8YMqIHeF7Mg4ZyH6+fGazJgVLttUY=
-----END
CERTIFICATE-----
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>

```
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
    <Configuration>Debug</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
    <Configuration>Release</Configuration>
    <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
    <Configuration>Release</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
</ItemGroup>
<ItemGroup>
  <ClCompile Include="..\..\programs\ssl\ssl_mail_client.c" />
</ItemGroup>
<ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">
    <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
</ItemGroup>
<PropertyGroup Label="Globals">
  <ProjectGuid>{7C4863A1-941A-C5AE-E1F9-30F062E4B2FD}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>ssl_mail_client</RootNamespace>
</PropertyGroup>
<Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
```

```
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')"
 Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup
 Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
   <PrecompiledHeader>
   </PrecompiledHeader>
   <WarningLevel>Level3</WarningLevel>
   <Optimization>Disabled</Optimization>
```

<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
<AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
</ClCompile>
<Link>
<SubSystem>Console</SubSystem>
<GenerateDebugInformation>true</GenerateDebugInformation>
<ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
<AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
</Link>
<ProjectReference>
<LinkLibraryDependencies>false</LinkLibraryDependencies>
</ProjectReference>
</ItemDefinitionGroup>
<ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
<ClCompile>
<PrecompiledHeader>
</PrecompiledHeader>
<WarningLevel>Level3</WarningLevel>
<Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
<AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
</ClCompile>
<Link>
<SubSystem>Console</SubSystem>
<GenerateDebugInformation>true</GenerateDebugInformation>
<ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
<AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
</Link>
<ProjectReference>
<LinkLibraryDependencies>false</LinkLibraryDependencies>
</ProjectReference>
</ItemDefinitionGroup>
<ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
<ClCompile>
<WarningLevel>Level3</WarningLevel>
<PrecompiledHeader>
</PrecompiledHeader>
<Optimization>MaxSpeed</Optimization>
<FunctionLevelLinking>true</FunctionLevelLinking>
<IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
<AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>

```
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
  </Link>
 </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
  <Import Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
-----BEGIN EC PARAMETERS-----
BggqhkjOPQMBBw==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIBx2xwapGbHTy79IbpJkc/w9LJXPKNG7gGRLPOGPQFI6oAoGCCqGSM49
AwEHoUQDQgAEEQ1wzSItaXq3rnYasGti7JV4LMZwetx7ucuZYPtVj67iGD8w/x6N
AD73lXcxS1Y4tffmxOPrRT2C9UqbDdVn1g==
-----END EC PRIVATE KEY-----
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
```

```
  <ProjectConfiguration Include="Debug|Win32">
    <Configuration>Debug</Configuration>
    <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
    <Configuration>Debug</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
    <Configuration>Release</Configuration>
    <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
    <Configuration>Release</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
</ItemGroup>
<ItemGroup>
  <ClCompile Include="..\..\programs\test\benchmark.c" />
</ItemGroup>
<ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">

    <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
</ItemGroup>
<PropertyGroup Label="Globals">
  <ProjectGuid>{90EFD9A4-C6B0-3EE8-1F06-0A0E0D55AEDA}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>benchmark</RootNamespace>
</PropertyGroup>
<Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
    <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
</PropertyGroup>
```

```
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
/>
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
   <PrecompiledHeader>
   </PrecompiledHeader>
```

```
    <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
     <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
   </Link>
   <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
   </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
   <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
   </Link>
   <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
   </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
```

<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
<AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
</ClCompile>
<Link>
<SubSystem>Console</SubSystem>
<GenerateDebugInformation>true</GenerateDebugInformation>
<EnableCOMDATFolding>true</EnableCOMDATFolding>
<OptimizeReferences>true</OptimizeReferences>
<AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
</Link>
</ItemDefinitionGroup>
<ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
<ClCompile>
<WarningLevel>Level3</WarningLevel>
<PrecompiledHeader>
</PrecompiledHeader>
<Optimization>MaxSpeed</Optimization>
<FunctionLevelLinking>true</FunctionLevelLinking>
<IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
<AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
</ClCompile>
<Link>
<SubSystem>Console</SubSystem>
<GenerateDebugInformation>true</GenerateDebugInformation>
<EnableCOMDATFolding>true</EnableCOMDATFolding>
<OptimizeReferences>true</OptimizeReferences>
<AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
</Link>
</ItemDefinitionGroup>
<Import
Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
<ImportGroup Label="ExtensionTargets">
</ImportGroup>
</Project>
-----BEGIN CERTIFICATE-----
MIIBzDCCAVOgAwIBAgIJAPejOupCJS65MAoGCCqGSM49BAMCMD4xCzAJBgNVBAYT
Ak5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBF
QyBDQTAeFw0xNDA0MDkxMTIyMjVaFw0yNDA0MDYxMTIyMjVaMD4xCzAJBgNVBAYT
Ak5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBF
QyBDQTB2MBAGByqGSM49AgEGBSuBBAAiA2IABMPaKzRBN1gvh1b+/Im6KUNLTuBu
ww5XUzM5WNRStJGVOQsj318XJGJI/BqVKc4sLYfCiFKAr9ZqqyHduNMcbli4yuiy
aY7zQa0pw7RfdadHb9UZKVVpmlM7ILRmFmAzHqMdMBswDAYDVR0TBAUwAwEB/zAL
BgNVHQ8EBAMCAQYwCgYIKoZIzj0EAwIDZwAwZAIwMKLVXB4YBQ0Ha4dEvFPcJtau

TS5Vd4UqG3xQ10YcJogweuqaGHSFgdnEUfoX+4p5AjApMnYXFfUjSmlyfJmTaswO
gaR5sUnnw33NA9j1ercem3asCYz6a8T0zo8/rR33XVU=
-----END CERTIFICATE-----
RSAES-OAEP Encryption Test Vector Int
pkcs1_rsaes_oaep_encrypt:1024:16:"bbf82f090682ce9c2338ac2b9da871f7368d07eed41043a440d6b6f07454f51fb8
dfbaaf035c02ab61ea48ceeb6fcd4876ed520d60e1ec4619719d8a5b8b807fafb8e0a3dfc737723ee6b4b7d93a2584ee6a
649d060953748834b2454598394ee0aab12d7b61a51f527a9a41f6c1687fe2537298ca2a8f5946f8e5fd091dbdcb":16:"
11":MBEDTLS_MD_SHA1:"d436e99569fd32a7c8a05bbc90d32c49":"aafd12f659cae63489b479e5076ddec2f06cb5
8f":"1253e04dc0a5397bb44a7ab87e9bf2a039a33d1e996fc82a94ccd30074c95df763722017069e5268da5d1c0b4f87
2cf653c11df82314a67968dfeae28def04bb6d84b1c31d654a1970e5783bd6eb96a024c2ca2f4a90fe9f2ef5c9c140e5bb
48da9536ad8700c84fc9130adea74e558d51a74ddf85d8b50de96838d6063e0955":0

RSAES-OAEP Encryption Test Vector Data just fits
pkcs1_rsaes_oaep_encrypt:1024:16:"bbf82f090682ce9c2338ac2b9da871f7368d07eed41043a440d6b6f07454f51fb8
dfbaaf035c02ab61ea48ceeb6fcd4876ed520d60e1ec4619719d8a5b8b807fafb8e0a3dfc737723ee6b4b7d93a2584ee6a
649d060953748834b2454598394ee0aab12d7b61a51f527a9a41f6c1687fe2537298ca2a8f5946f8e5fd091dbdcb":16:"
11":MBEDTLS_MD_SHA1:"d436e99569fd32a7c8a05bbc90d32c49d436e99569fd32a7c8a05bbc90d32c49d436e99
569fd32a7c8a05bbc90d32c49d436e99569fd32a7c8a05bbc90d32c49d436e99569fd32a7c8a05bbc90d32c49d436e99
569fd":"aafd12f659cae63489b479e5076ddec2f06cb58f":"3082f2288fff275213d53168f0a272573cff81837c249dc1f3
80a12ac124c8f217b700708a1ce7dce154265f31a126ebdd9ed3ef9145ae29124a25f4e65aa52c5a9ff34f6cf4de9ba937a
e406dc7d1f277af4f6fb7ea73bfbab2bd397b6b2c53570e173ffcf3b9f0bb96837623a4f87bd81b41446c59e681a2f3da8
1239e9bdf":0

RSAES-OAEP
Encryption Test Vector Data too long
pkcs1_rsaes_oaep_encrypt:1024:16:"bbf82f090682ce9c2338ac2b9da871f7368d07eed41043a440d6b6f07454f51fb8
dfbaaf035c02ab61ea48ceeb6fcd4876ed520d60e1ec4619719d8a5b8b807fafb8e0a3dfc737723ee6b4b7d93a2584ee6a
649d060953748834b2454598394ee0aab12d7b61a51f527a9a41f6c1687fe2537298ca2a8f5946f8e5fd091dbdcb":16:"
11":MBEDTLS_MD_SHA1:"d436e99569fd32a7c8a05bbc90d32c49d436e99569fd32a7c8a05bbc90d32c49d436e99
569fd32a7c8a05bbc90d32c49d436e99569fd32a7c8a05bbc90d32c49d436e99569fd32a7c8a05bbc90d32c49d436e99
569fd00":"aafd12f659cae63489b479e5076ddec2f06cb58f":"1253e04dc0a5397bb44a7ab87e9bf2a039a33d1e996fc8
2a94ccd30074c95df763722017069e5268da5d1c0b4f872cf653c11df82314a67968dfeae28def04bb6d84b1c31d654a1
970e5783bd6eb96a024c2ca2f4a90fe9f2ef5c9c140e5bb48da9536ad8700c84fc9130adea74e558d51a74ddf85d8b50de
96838d6063e0955":MBEDTLS_ERR_RSA_BAD_INPUT_DATA

RSAES-OAEP
Encryption Test Vector 1_1
pkcs1_rsaes_oaep_encrypt:1024:16:"a8b3b284af8eb50b387034a860f146c4919f318763cd6c5598c8ae4811a1e0abc4
c7e0b082d693a5e7fced675cf4668512772c0cbc64a742c6c630f533c8cc72f62ae833c40bf25842e984bb78bdbf97c01
07d55bdb662f5c4e0fab9845cb5148ef7392dd3aaff93ae1e6b667bb3d4247616d4f5ba10d4cfd226de88d39f16fb":16:"
010001":MBEDTLS_MD_SHA1:"6628194e12073db03ba94cda9ef9532397d50dba79b987004afefe34":"18b776ea2
1069d69776a33e96bad48e1dda0a5ef":"354fe67b4a126d5d35fe36c777791a3f7ba13def484e2d3908aff722fad468fb2
1696de95d0be911c2d3174f8afcc201035f7b6d8e69402de5451618c21a535fa9d7bfc5b8dd9fc243f8cf927db31322d6
e881eaa91a996170e657a05a266426d98c88003f8477c1227094a0d9fa1e8c4024309ce1ecccb5210035d47ac72e8a":0

RSAES-OAEP
Encryption Test Vector 1_2
pkcs1_rsaes_oaep_encrypt:1024:16:"a8b3b284af8eb50b387034a860f146c4919f318763cd6c5598c8ae4811a1e0abc4

c7e0b082d693a5e7fced675cf4668512772c0cbc64a742c6c630f533c8cc72f62ae833c40bf25842e984bb78bdbf97c01
07d55bdb662f5c4e0fab9845cb5148ef7392dd3aaff93ae1e6b667bb3d4247616d4f5ba10d4cfd226de88d39f16fb":16:"
010001":MBEDTLS_MD_SHA1:"750c4047f547e8e41411856523298ac9bae245efaf1397fbe56f9dd5":"0cc742ce4a
9b7f32f951bcb251efd925fe4fe35f":"640db1acc58e0568fe5407e5f9b701dff8c3c91e716c536fc7fcec6cb5b71c11659
88d4a279e1577d730fc7a29932e3f00c81515236d8d8e31017a7a09df4352d904cdeb79aa583adcc31ea698a4c05283d
aba9089be5491f67c1a4ee48dc74bbbe6643aef846679b4cb395a352d5ed115912df696ffe0702932946d71492b44":0

RSAES-OAEP Encryption Test Vector 1_3
pkcs1_rsaes_oaep_encrypt:1024:16:"a8b3b284af8eb50b387034a860f146c4919f318763cd6c5598c8ae4811a1e0abc4
c7e0b082d693a5e7fced675cf4668512772c0cbc64a742c6c630f533c8cc72f62ae833c40bf25842e984bb78bdbf97c01
07d55bdb662f5c4e0fab9845cb5148ef7392dd3aaff93ae1e6b667bb3d4247616d4f5ba10d4cfd226de88d39f16fb":16:"
010001":MBEDTLS_MD_SHA1:"d94ae0832e6445ce42331cb06d531a82b1db4baad30f746dc916df24d4e3c2451fff
59a6423eb0e1d02d4fe646cf699dfd818c6e97b051":"2514df4695755a67b288eaf4905c36eec66fd2fd":"423736ed035
f6026af276c35c0b3741b365e5f76ca091b4e8c29e2f0befee603595aa8322d602d2e625e95eb81b2f1c9724e822eca76d
b8618cf09c5343503a4360835b5903bc637e3879fb05e0ef32685d5aec5067cd7cc96fe4b2670b6eac3066b1fcf5686b6
8589aafb7d629b02d8f8625ca3833624d4800fb081b1cf94eb":0

RSAES-OAEP
Encryption Test Vector 1_4
pkcs1_rsaes_oaep_encrypt:1024:16:"a8b3b284af8eb50b387034a860f146c4919f318763cd6c5598c8ae4811a1e0abc4
c7e0b082d693a5e7fced675cf4668512772c0cbc64a742c6c630f533c8cc72f62ae833c40bf25842e984bb78bdbf97c01
07d55bdb662f5c4e0fab9845cb5148ef7392dd3aaff93ae1e6b667bb3d4247616d4f5ba10d4cfd226de88d39f16fb":16:"
010001":MBEDTLS_MD_SHA1:"52e650d98e7f2a048b4f86852153b97e01dd316f346a19f67a85":"c4435a3e1a18a
68b6820436290a37cefb85db3fb":"45ead4ca551e662c9800f1aca8283b0525e6abae30be4b4aba762fa40fd3d38e22ab
efc69794f6ebbbc05ddbb11216247d2f412fd0fba87c6e3acd888813646fd0e48e785204f9c3f73d6d8239562722dddd8
771fec48b83a31ee6f592c4cfd4bc88174f3b13a112aae3b9f7b80e0fc6f7255ba880dc7d8021e22ad6a85f0755":0

RSAES-OAEP
Encryption Test Vector 1_5
pkcs1_rsaes_oaep_encrypt:1024:16:"a8b3b284af8eb50b387034a860f146c4919f318763cd6c5598c8ae4811a1e0abc4
c7e0b082d693a5e7fced675cf4668512772c0cbc64a742c6c630f533c8cc72f62ae833c40bf25842e984bb78bdbf97c01
07d55bdb662f5c4e0fab9845cb5148ef7392dd3aaff93ae1e6b667bb3d4247616d4f5ba10d4cfd226de88d39f16fb":16:"
010001":MBEDTLS_MD_SHA1:"8da89fd9e5f974a29feffb462b49180f6cf9e802":"b318c42df3be0f83fea823f5a7b4
7ed5e425a3b5":"36f6e34d94a8d34daacba33a2139d00ad85a9345a86051e73071620056b920e219005855a213a0f23
897cdcd731b45257c777fe908202befdd0b58386b1244ea0cf539a05d5d10329da44e13030fd760dcd644cfef2094d191
0d3f433e1c7c6dd18bc1f2df7f643d662fb9dd37ead9059190f4fa66ca39e869c4eb449cbdc439":0

RSAES-OAEP
Encryption Test Vector 1_6
pkcs1_rsaes_oaep_encrypt:1024:16:"a8b3b284af8eb50b387034a860f146c4919f318763cd6c5598c8ae4811a1e0abc4
c7e0b082d693a5e7fced675cf4668512772c0cbc64a742c6c630f533c8cc72f62ae833c40bf25842e984bb78bdbf97c01
07d55bdb662f5c4e0fab9845cb5148ef7392dd3aaff93ae1e6b667bb3d4247616d4f5ba10d4cfd226de88d39f16fb":16:"
010001":MBEDTLS_MD_SHA1:"26521050844271":"e4ec0982c2336f3a677f6a356174eb0ce887abc2":"42cee2617
b1ecea4db3f4829386fbd61dafbf038e180d837c96366df24c097b4ab0fac6bdf590d821c9f10642e681ad05b8d78b378
c0f46ce2fad63f74e0ad3df06b075d7eb5f5636f8d403b9059ca761b5c62bb52aa45002ea70baace08ded243b9d8cbd62
a68ade265832b56564e43a6fa42ed199a099769742df1539e8255":0

RSAES-OAEP Encryption Test Vector 2_1

pkcs1_rsaes_oaep_encrypt:1025:16:"01947c7fce90425f47279e70851f25d5e62316fe8a1df19371e3e628e260543e49
01ef6081f68c0b8141190d2ae8daba7d1250ec6db636e944ec3722877c7c1d0a67f14b1694c5f0379451a43e49a32dde8
3670b73da91a1c99bc23b436a60055c610f0baf99c1a079565b95a3f1526632d1d4da60f20eda25e653c4f002766f45":
16:"010001":MBEDTLS_MD_SHA1:"8ff00caa605c702830634d9a6c3d42c652b58cf1d92fec570beee7":"8c407b5e
c2899e5099c53e8ce793bf94e71b1782":"0181af8922b9fcb4d79d92ebe19815992fc0c1439d8bcd491398a0f4ad3a32
9a5bd9385560db532683c8b7da04e4b12aed6aacdf471c34c9cda891addcc2df3456653aa6382e9ae59b54455257eb09
9d562bbe10453f2b6d13c59c02e10f1f8abb5da0d0570932dacf2d0901db729d0fefcc054e70968ea540c81b04bcaefe72
0e":0

RSAES-OAEP
Encryption Test Vector 2_2
pkcs1_rsaes_oaep_encrypt:1025:16:"01947c7fce90425f47279e70851f25d5e62316fe8a1df19371e3e628e260543e49
01ef6081f68c0b8141190d2ae8daba7d1250ec6db636e944ec3722877c7c1d0a67f14b1694c5f0379451a43e49a32dde8
3670b73da91a1c99bc23b436a60055c610f0baf99c1a079565b95a3f1526632d1d4da60f20eda25e653c4f002766f45":
16:"010001":MBEDTLS_MD_SHA1:"2d":"b600cf3c2e506d7f16778c910d3a8b003eee61d5":"018759ff1df63b2792
410562314416a8aeaf2ac634b46f940ab82d64dbf165eee33011da749d4bab6e2fcd18129c9e49277d8453112b429a22
2a8471b070993998e758861c4d3f6d749d91c4290d332c7a4ab3f7ea35ff3a07d497c955ff0ffc95006b62c6d296810d9
bfab024196c7934012c2df978ef299aba239940cba10245":0

RSAES-OAEP
Encryption Test Vector 2_3
pkcs1_rsaes_oaep_encrypt:1025:16:"01947c7fce90425f47279e70851f25d5e62316fe8a1df19371e3e628e260543e49
01ef6081f68c0b8141190d2ae8daba7d1250ec6db636e944ec3722877c7c1d0a67f14b1694c5f0379451a43e49a32dde8
3670b73da91a1c99bc23b436a60055c610f0baf99c1a079565b95a3f1526632d1d4da60f20eda25e653c4f002766f45":
16:"010001":MBEDTLS_MD_SHA1:"74fc88c51bc90f77af9d5e9a4a70133d4b4e0b34da3c37c7ef8e":"a73768aeeaa
91f9d8c1ed6f9d2b63467f07ccae3":"018802bab04c60325e81c4962311f2be7c2adce93041a00719c88f957575f2c79f
1b7bc8ced115c706b311c08a2d986ca3b6a9336b147c29c6f229409ddec651bd1fdd5a0b7f610c9937fdb4a3a762364b
8b3206b4ea485fd098d08f63d4aa8bb2697d027b750c32d7f74eaf5180d2e9b66b17cb2fa55523bc280da10d14be2053
":0

RSAES-OAEP Encryption Test Vector 2_4
pkcs1_rsaes_oaep_encrypt:1025:16:"01947c7fce90425f47279e70851f25d5e62316fe8a1df19371e3e628e260543e49
01ef6081f68c0b8141190d2ae8daba7d1250ec6db636e944ec3722877c7c1d0a67f14b1694c5f0379451a43e49a32dde8
3670b73da91a1c99bc23b436a60055c610f0baf99c1a079565b95a3f1526632d1d4da60f20eda25e653c4f002766f45":
16:"010001":MBEDTLS_MD_SHA1:"a7eb2a5036931d27d4e891326d99692ffadda9bf7efd3e34e622c4adc085f721
dfe885072c78a203b151739be540fa8c153a10f00a":"9a7b3b0e708bd96f8190ecab4fb9b2b3805a8156":"00a4578cbc
176318a638fba7d01df15746af44d4f6cd96d7e7c495cbf425b09c649d32bf886da48fbaf989a2117187cafb1fb5803176
90e3ccd446920b7af82b31db5804d87d01514acbfa9156e782f867f6bed9449e0e9a2c09bcecc6aa087636965e34b3ec7
66f2fe2e43018a2fddeb140616a0e9d82e5331024ee0652fc7641":0

RSAES-OAEP
Encryption Test Vector 2_5
pkcs1_rsaes_oaep_encrypt:1025:16:"01947c7fce90425f47279e70851f25d5e62316fe8a1df19371e3e628e260543e49
01ef6081f68c0b8141190d2ae8daba7d1250ec6db636e944ec3722877c7c1d0a67f14b1694c5f0379451a43e49a32dde8
3670b73da91a1c99bc23b436a60055c610f0baf99c1a079565b95a3f1526632d1d4da60f20eda25e653c4f002766f45":
16:"010001":MBEDTLS_MD_SHA1:"2ef2b066f854c33f3bdcbb5994a435e73d6c6c":"eb3cebbc4adc16bb48e88c8a
ec0e34af7f427fd3":"00ebc5f5fda77cfdad3c83641a9025e77d72d8a6fb33a810f5950f8d74c73e8d931e8634d86ab124
6256ae07b6005b71b7f2fb98351218331ce69b8ffbdc9da08bbc9c704f876deb9df9fc2ec065cad87f9090b07acc17aa7f

997b27aca48806e897f771d95141fe4526d8a5301b678627efab707fd40fbebd6e792a25613e7aec":0

RSAES-OAEP
Encryption Test Vector 2_6
pkcs1_rsaes_oaep_encrypt:1025:16:"01947c7fce90425f47279e70851f25d5e62316fe8a1df19371e3e628e260543e49
01ef6081f68c0b8141190d2ae8daba7d1250ec6db636e944ec3722877c7c1d0a67f14b1694c5f0379451a43e49a32dde8
3670b73da91a1c99bc23b436a60055c610f0baf99c1a079565b95a3f1526632d1d4da60f20eda25e653c4f002766f45":
16:"010001":MBEDTLS_MD_SHA1:"8a7fb344c8b6cb2cf2ef1f643f9a3218f6e19bba89c0":"4c45cf4d57c98e3d6d2
095adc51c489eb50dff84":"010839ec20c27b9052e55befb9b77e6fc26e9075d7a54378c646abdf51e445bd5715de817
89f56f1803d9170764a9e93cb78798694023ee7393ce04bc5d8f8c5a52c171d43837e3aca62f609eb0aa5ffb0960ef0419
8dd754f57f7fbe6abf765cf118b4ca443b23b5aab266f952326ac4581100644325f8b721acd5d04ff14ef3a":0

RSAES-OAEP
Encryption Example 3_1
pkcs1_rsaes_oaep_encrypt:1026:16:"02b58fec039a860700a4d7b6462f93e6cdd491161ddd74f4e810b40e3c1652006
a5c277b2774c11305a4cbab5a78efa57e17a86df7a3fa36fc4b1d2249f22ec7c2dd6a463232accea906d66ebe80b5704b1
0729da6f833234abb5efdd4a292cbfad33b4d33fa7a14b8c397b56e3acd21203428b77cdfa33a6da706b3d8b0fc43e9":1
6:"010001":MBEDTLS_MD_SHA1:"087820b569e8fa8d":"8ced6b196290805790e909074015e6a20b0c4894":"026
a0485d96aebd96b4382085099b962e6a2bdec3d90c8db625e14372de85e2d5b7baab65c8faf91bb5504fb495afce5c988
b3f6a52e20e1d6cbd3566c5cd1f2b8318bb542cc0ea25c4aab9932afa20760eaddec784396a07ea0ef24d4e6f4d37e5052
a7a31e146aa480a111bbe926401307e00f410033842b6d82fe5ce4dfae80":0

RSAES-OAEP Encryption Example 3_2
pkcs1_rsaes_oaep_encrypt:1026:16:"02b58fec039a860700a4d7b6462f93e6cdd491161ddd74f4e810b40e3c1652006
a5c277b2774c11305a4cbab5a78efa57e17a86df7a3fa36fc4b1d2249f22ec7c2dd6a463232accea906d66ebe80b5704b1
0729da6f833234abb5efdd4a292cbfad33b4d33fa7a14b8c397b56e3acd21203428b77cdfa33a6da706b3d8b0fc43e9":1
6:"010001":MBEDTLS_MD_SHA1:"4653acaf171960b01f52a7be63a3ab21dc368ec43b50d82ec3781e04":"b4291d
6567550848cc156967c809baab6ca507f0":"024db89c7802989be0783847863084941bf209d761987e38f97cb5f6f1bc
88da72a50b73ebaf11c879c4f95df37b850b8f65d7622e25b1b889e80fe80baca2069d6e0e1d829953fc459069de98ea9
798b451e557e99abf8fe3d9ccf9096ebbf3e5255d3b4e1c6d2ecadf067a359eea86405acd47d5e165517ccafd47d6dbee4
bf5":0

RSAES-OAEP
Encryption Example 3_3
pkcs1_rsaes_oaep_encrypt:1026:16:"02b58fec039a860700a4d7b6462f93e6cdd491161ddd74f4e810b40e3c1652006
a5c277b2774c11305a4cbab5a78efa57e17a86df7a3fa36fc4b1d2249f22ec7c2dd6a463232accea906d66ebe80b5704b1
0729da6f833234abb5efdd4a292cbfad33b4d33fa7a14b8c397b56e3acd21203428b77cdfa33a6da706b3d8b0fc43e9":1
6:"010001":MBEDTLS_MD_SHA1:"d94cd0e08fa404ed89":"ce8928f6059558254008badd9794fadcd2fd1f65":"023
9bce681032441528877d6d1c8bb28aa3bc97f1df5845636189957976838 44ca86664732f4bed7a0aab083aaabfb7238f
582e30958c2024e44e57043b97950fd543da977c90cdde5337d618442f99e60d7783ab59ce6dd9d69c47ad1e962bec22
d05895cff8d3f64ed5261d92b2678510393484990ba3f7f06818ae6ffce8a3a":0

RSAES-OAEP
Encryption Example 3_4
pkcs1_rsaes_oaep_encrypt:1026:16:"02b58fec039a860700a4d7b6462f93e6cdd491161ddd74f4e810b40e3c1652006
a5c277b2774c11305a4cbab5a78efa57e17a86df7a3fa36fc4b1d2249f22ec7c2dd6a463232accea906d66ebe80b5704b1
0729da6f833234abb5efdd4a292cbfad33b4d33fa7a14b8c397b56e3acd21203428b77cdfa33a6da706b3d8b0fc43e9":1
6:"010001":MBEDTLS_MD_SHA1:"6cc641b6b61e6f963974dad23a9013284ef1":"6e2979f52d6814a57d83b09005

4888f119a5b9a3":"02994c62afd76f498ba1fd2cf642857fca81f4373cb08f1cbaee6f025c3b512b42c3e8779113476648
039dbe0493f9246292fac28950600e7c0f32edf9c81b9dec45c3bde0cc8d8847590169907b7dc5991ceb29bb0714d613
d96df0f12ec5d8d3507c8ee7ae78dd83f216fa61de100363aca48a7e914ae9f42ddfbe943b09d9a0":0

RSAES-OAEP Encryption Example 3_5
pkcs1_rsaes_oaep_encrypt:1026:16:"02b58fec039a860700a4d7b6462f93e6cdd491161ddd74f4e810b40e3c1652006
a5c277b2774c11305a4cbab5a78efa57e17a86df7a3fa36fc4b1d2249f22ec7c2dd6a463232accea906d66ebe80b5704b1
0729da6f833234abb5efdd4a292cbfad33b4d33fa7a14b8c397b56e3acd21203428b77cdfa33a6da706b3d8b0fc43e9":1
6:"010001":MBEDTLS_MD_SHA1:"df5151832b61f4f25891fb4172f328d2eddf8371ffcfdbe997939295f30eca6918
017cfda1153bf7a6af87593223":"2d760bfe38c59de34cdc8b8c78a38e66284a2d27":"0162042ff6969592a616703181
1a239834ce638abf54fec8b99478122afe2ee67f8c5b18b0339805bfdbc5a4e6720b37c59cfba942464c597ff532a11982
1545fd2e59b114e61daf71820529f5029cf524954327c34ec5e6f5ba7efcc4de943ab8ad4ed787b1454329f70db798a3a
8f4d92f8274e2b2948ade627ce8ee33e43c60":0

RSAES-OAEP
Encryption Example 3_6
pkcs1_rsaes_oaep_encrypt:1026:16:"02b58fec039a860700a4d7b6462f93e6cdd491161ddd74f4e810b40e3c1652006
a5c277b2774c11305a4cbab5a78efa57e17a86df7a3fa36fc4b1d2249f22ec7c2dd6a463232accea906d66ebe80b5704b1
0729da6f833234abb5efdd4a292cbfad33b4d33fa7a14b8c397b56e3acd21203428b77cdfa33a6da706b3d8b0fc43e9":1
6:"010001":MBEDTLS_MD_SHA1:"3c3bad893c544a6d520ab022319188c8d504b7a788b850903b85972eaa18552e
1134a7ad6098826254ff7ab672b3d8eb3158fac6d4cbaef1":"f174779c5fd3cfe007badcb7a36c9b55bfcfbf0e":"001120
51e75d064943bc4478075e43482fd59cee0679de6893eec3a943daa490b9691c93dfc0464b6623b9f3dbd3e70083264f
034b374f74164e1a00763725e574744ba0b9db83434f31df96f6e2a26f6d8eba348bd4686c2238ac07c37aac3785d1c7e
ea2f819fd91491798ed8e9cef5e43b781b0e0276e37c43ff9492d005730":0

RSAES-OAEP
Encryption Example 4_1
pkcs1_rsaes_oaep_encrypt:1027:16:"051240b6cc0004fa48d0134671c078c7c8dec3b3e2f25bc2564467339db38853d
06b85eea5b2de353bff42ac2e46bc97fae6ac9618da9537a5c8f553c1e357625991d6108dcd7885fb3a25413f53efcad94
8cb35cd9b9ae9c1c67626d113d57dde4c5bea76bb5bb7de96c00d07372e9685a6d75cf9d239fa148d70931b5f3fb039":
16:"010001":MBEDTLS_MD_SHA1:"4a86609534ee434a6cbca3f7e962e76d455e3264c19f605f6e5ff6137c65c56d7
fb344cd52bc93374f3d166c9f0c6f9c506bad19330972d2":"1cac19ce993def55f98203f6852896c95ccca1f3":"04cce19
614845e094152a3fe18e54e3330c44e5efbc64ae16886cb1869014cc5781b1f8f9e045384d0112a135ca0d12e9c88a8e4
063416deaae3844f60d6e96fe155145f4525b9a34431ca3766180f70e15a5e5d8e8b1a516ff870609f13f896935ced1882
79a58ed13d07114277d75c6568607e0ab092fd803a223e4a8ee0b1a8":0

RSAES-OAEP
Encryption Example 4_2
pkcs1_rsaes_oaep_encrypt:1027:16:"051240b6cc0004fa48d0134671c078c7c8dec3b3e2f25bc2564467339db38853d
06b85eea5b2de353bff42ac2e46bc97fae6ac9618da9537a5c8f553c1e357625991d6108dcd7885fb3a25413f53efcad94
8cb35cd9b9ae9c1c67626d113d57dde4c5bea76bb5bb7de96c00d07372e9685a6d75cf9d239fa148d70931b5f3fb039":
16:"010001":MBEDTLS_MD_SHA1:"b0adc4f3fe11da59ce992773d9059943c03046497ee9d9f9a06df1166db46d98
f58d27ec074c02eee6cbe2449c8b9fc5080c5c3f4433092512ec46aa793743c8":"f545d5897585e3db71aa0cb8da76c51
d032ae963":"0097b698c6165645b303486fbf5a2a4479c0ee85889b541a6f0b858d6b6597b13b854eb4f839af03399a8
0d79bda6578c841f90d645715b280d37143992dd186c80b949b775cae97370e4ec97443136c6da484e970ffdb1323a20
847821d3b18381de13bb49aaea66530c4a4b8271f3eae172cd366e07e6636f1019d2a28aed15e":0

RSAES-OAEP Encryption Example 4_3

pkcs1_rsaes_oaep_encrypt:1027:16:"051240b6cc0004fa48d0134671c078c7c8dec3b3e2f25bc2564467339db38853d06b85eea5b2de353bff42ac2e46bc97fae6ac9618da9537a5c8f553c1e357625991d6108dcd7885fb3a25413f53efcad948cb35cd9b9ae9c1c67626d113d57dde4c5bea76bb5bb7de96c00d07372e9685a6d75cf9d239fa148d70931b5f3fb039":16:"010001":MBEDTLS_MD_SHA1:"bf6d42e701707b1d0206b0c8b45a1c72641ff12889219a82bdea965b5e79a96b0d0163ed9d578ec9ada20f2fbcf1ea3c4089d83419ba81b0c60f3606da99":"ad997feef730d6ea7be60d0dc52e72eacbfdd275":"0301f935e9c47abcb48acbbe09895d9f5971af14839da4ff95417ee453d1fd77319072bb7297e1b55d7561cd9d1bb24c1a9a37c619864308242804879d86ebd001dce5183975e1506989b70e5a83434154d5cbfd6a24787e60eb0c658d2ac193302d1192c6e622d4a12ad4b53923bca246df31c6395e37702c6a78ae081fb9d065":0

RSAES-OAEP
Encryption Example 4_4
pkcs1_rsaes_oaep_encrypt:1027:16:"051240b6cc0004fa48d0134671c078c7c8dec3b3e2f25bc2564467339db38853d06b85eea5b2de353bff42ac2e46bc97fae6ac9618da9537a5c8f553c1e357625991d6108dcd7885fb3a25413f53efcad948cb35cd9b9ae9c1c67626d113d57dde4c5bea76bb5bb7de96c00d07372e9685a6d75cf9d239fa148d70931b5f3fb039":16:"010001":MBEDTLS_MD_SHA1:"fb2ef112f5e766eb94019297934794f7be2f6fc1c58e":"136454df5730f73c807a7e40d8c1a312ac5b9dd3":"02d110ad30afb727beb691dd0cf17d0af1a1e7fa0cc040ec1a4ba26a42c59d0a796a2e22c8f357ccc98b6519aceb682e945e62cb734614a529407cd452bee3e44fece8423cc19e55548b8b994b849c7ecde4933e76037e1d0ce44275b08710c68e430130b929730ed77e09b015642c5593f04e4ffb9410798102a8e96ffdfe11e4":0

RSAES-OAEP
Encryption Example 4_5
pkcs1_rsaes_oaep_encrypt:1027:16:"051240b6cc0004fa48d0134671c078c7c8dec3b3e2f25bc2564467339db38853d06b85eea5b2de353bff42ac2e46bc97fae6ac9618da9537a5c8f553c1e357625991d6108dcd7885fb3a25413f53efcad948cb35cd9b9ae9c1c67626d113d57dde4c5bea76bb5bb7de96c00d07372e9685a6d75cf9d239fa148d70931b5f3fb039":16:"010001":MBEDTLS_MD_SHA1:"28ccd447bb9e85166dabb9e5b7d1adadc4b9d39f204e96d5e440ce9ad928bc1c2284":"bca8057f824b2ea257f2861407eef63d33208681":"00dbb8a7439d90efd919a377c54fae8fe11ec58c3b858362e23ad1b8a44310799066b99347aa525691d2adc58d9b06e34f288c170390c5f0e11c0aa3645959f18ee79e8f2be8d7ac5c23d061f18dd74b8c5f2a58fcb5eb0c54f99f01a83247568292536583340948d7a8c97c4acd1e98d1e29dc320e97a260532a8aa7a758a1ec2":0

RSAES-OAEP
Encryption Example 4_6
pkcs1_rsaes_oaep_encrypt:1027:16:"051240b6cc0004fa48d0134671c078c7c8dec3b3e2f25bc2564467339db38853d06b85eea5b2de353bff42ac2e46bc97fae6ac9618da9537a5c8f553c1e357625991d6108dcd7885fb3a25413f53efcad948cb35cd9b9ae9c1c67626d113d57dde4c5bea76bb5bb7de96c00d07372e9685a6d75cf9d239fa148d70931b5f3fb039":16:"010001":MBEDTLS_MD_SHA1:"f22242751ec6b1":"2e7e1e17f647b5ddd033e15472f90f6812f3ac4e":"00a5ffa4768c8bbecaee2db77e8f2eec99595933545520835e5ba7db9493d3e17cddefe6a5f567624471908db4e2d83a0fbee60608fc84049503b2234a07dc83b27b22847ad8920ff42f674ef79b76280b00233d2b51b8cb2703a9d42bfbc8250c96ec32c051e57f1b4ba528db89c37e4c54e27e6e64ac69635ae887d9541619a9":0

RSAES-OAEP Encryption Example 5_1
pkcs1_rsaes_oaep_encrypt:1028:16:"0aadf3f9c125e5d891f31ac448e993defe580f802b45f9d7f22ba5021e9c47576b5a1e68031ba9db4e6dabe4d96a1d6f3d267268cff408005f118efcadb99888d1c234467166b2a2b849a05a889c060ac0da0c5fae8b55f309ba62e703742fa0326f2d10b011021489ff497770190d895fd39f52293c39efd73a698bdab9f10ed9":16:"010001":MBEDTLS_MD_SHA1:"af71a901e3a61d3132f0fc1fdb474f9ea6579257ffc24d164170145b3dbde8":"44c92e283f77b9499c603d963660c87d2f939461":"036046a4a47d9ed3ba9a89139c105038eb7492b05a5d68bfd53accff4597f7a68651b47b4a4627d927e485eed7b4566420e8b409879e5d606eae251d22a5df799f7920bfc117b992572a53b1263146bcea03385cc5e853c9a101c8c3e1bda31a519807496c6cb5e5efb408823a352b8fa0661fb664efadd593deb99fff5

ed000e5":0

RSAES-OAEP
Encryption Example 5_2
pkcs1_rsaes_oaep_encrypt:1028:16:"0aadf3f9c125e5d891f31ac448e993defe580f802b45f9d7f22ba5021e9c47576b5a1e68031ba9db4e6dabe4d96a1d6f3d267268cff408005f118efcadb99888d1c234467166b2a2b849a05a889c060ac0da0c5fae8b55f309ba62e703742fa0326f2d10b011021489ff497770190d895fd39f52293c39efd73a698bdab9f10ed9":16:"010001":MBEDTLS_MD_SHA1:"a3b844a08239a8ac41605af17a6cfda4d350136585903a417a79268760519a4b4ac3303ec73f0f87cfb32399":"cb28f5860659fceee49c3eeafce625a70803bd32":"03d6eb654edce615bc59f455265ed4e5a18223cbb9be4e4069b473804d5de96f54dcaaa603d049c5d94aa1470dfcd2254066b7c7b61ff1f6f6770e3215c51399fd4e34ec5082bc48f089840ad04354ae66dc0f1bd18e461a33cc1258b443a2837a6df26759aa2302334986f87380c9cc9d53be9f99605d2c9a97da7b0915a4a7ad":0

RSAES-OAEP
Encryption Example 5_3
pkcs1_rsaes_oaep_encrypt:1028:16:"0aadf3f9c125e5d891f31ac448e993defe580f802b45f9d7f22ba5021e9c47576b5a1e68031ba9db4e6dabe4d96a1d6f3d267268cff408005f118efcadb99888d1c234467166b2a2b849a05a889c060ac0da0c5fae8b55f309ba62e703742fa0326f2d10b011021489ff497770190d895fd39f52293c39efd73a698bdab9f10ed9":16:"010001":MBEDTLS_MD_SHA1:"308b0ecbd2c76cb77fc6f70c5edd233fd2f20929d629f026953bb62a8f4a3a314bde195de85b5f816da2aab074d26cb6acddf323ae3b9c678ac3cf12fbdde7":"2285f40d770482f9a9efa2c72cb3ac55716dc0ca":"0770952181649f9f9f07ff626ff3a22c35c462443d905d456a9fd0bff43cac2ca7a9f554e9478b9acc3ac838b02040ffd3e1847de2e4253929f9dd9ee4044325a9b05cabb808b2ee840d34e15d105a3f1f7b27695a1a07a2d73fe08ecaaa3c9c9d4d5a89ff890d54727d7ae40c0ec1a8dd86165d8ee2c6368141016a48b55b6967":0

RSAES-OAEP
Encryption Example 5_4
pkcs1_rsaes_oaep_encrypt:1028:16:"0aadf3f9c125e5d891f31ac448e993defe580f802b45f9d7f22ba5021e9c47576b5a1e68031ba9db4e6dabe4d96a1d6f3d267268cff408005f118efcadb99888d1c234467166b2a2b849a05a889c060ac0da0c5fae8b55f309ba62e703742fa0326f2d10b011021489ff497770190d895fd39f52293c39efd73a698bdab9f10ed9":16:"010001":MBEDTLS_MD_SHA1:"15c5b9ee1185":"49fa45d3a78dd10dfd577399d1eb00af7eed5513":"0812b76768ebcb642d040258e5f4441a018521bd96687e6c5e899fcd6c17588ff59a82cc8ae03a4b45b31299af1788c329f7dcd285f8cf4ced82606b97612671a45bedca133442144d1617d114f802857f0f9d739751c57a3f9ee400912c61e2e6992be031a43dd48fa6ba14eef7c422b5edc4e7afa04fdd38f402d1c8bb719abf":0

RSAES-OAEP Encryption Example 5_5
pkcs1_rsaes_oaep_encrypt:1028:16:"0aadf3f9c125e5d891f31ac448e993defe580f802b45f9d7f22ba5021e9c47576b5a1e68031ba9db4e6dabe4d96a1d6f3d267268cff408005f118efcadb99888d1c234467166b2a2b849a05a889c060ac0da0c5fae8b55f309ba62e703742fa0326f2d10b011021489ff497770190d895fd39f52293c39efd73a698bdab9f10ed9":16:"010001":MBEDTLS_MD_SHA1:"21026e6800c7fa728fcaaba0d196ae28d7a2ac4ffd8abce794f0985f60c8a6737277365d3fea11db8923a2029a":"f0287413234cc5034724a094c4586b87aff133fc":"07b60e14ec954bfd29e60d0047e789f51d57186c63589903306793ced3f68241c743529aba6a6374f92e19e0163efa33697e196f7661dfaaa47aac6bde5e51deb507c72c589a2ca1693d96b1460381249b2cdb9eac44769f2489c5d3d2f99f0ee3c7ee5bf64a5ac79c42bd433f149be8cb59548361640595513c97af7bc2509723":0

RSAES-OAEP
Encryption Example 5_6
pkcs1_rsaes_oaep_encrypt:1028:16:"0aadf3f9c125e5d891f31ac448e993defe580f802b45f9d7f22ba5021e9c47576b5a1e68031ba9db4e6dabe4d96a1d6f3d267268cff408005f118efcadb99888d1c234467166b2a2b849a05a889c060ac0da

0c5fae8b55f309ba62e703742fa0326f2d10b011021489ff497770190d895fd39f52293c39efd73a698bdab9f10ed9":16:
"010001":MBEDTLS_MD_SHA1:"541e37b68b6c8872b84c02":"d9fba45c96f21e6e26d29eb2cdcb6585be9cb341":"
08c36d4dda33423b2ed6830d85f6411ba1dcf470a1fae0ebefee7c089f256cef74cb96ea69c38f60f39abee44129bcb4c9
2de7f797623b20074e3d9c2899701ed9071e1efa0bdd84d4c3e5130302d8f0240baba4b84a71cc032f2235a5ff0fae277
c3e8f9112bef44c9ae20d175fc9a4058bfc930ba31b02e2e4f444483710f24a":0

RSAES-OAEP
Encryption Example 6_1
pkcs1_rsaes_oaep_encrypt:1029:16:"12b17f6dad2ecd19ff46dc13f7860f09e0e0cfb677b38a52592305ceaf022c166db
90d04ac29e33f7dd12d9faf66e0816bb63ead267cc7d46c17c37be214bca2a22d723a64e44407436b6fc965729aefc255
4f376cd5dcea68293780a62bf39d0029485a160bbb9e5dc0972d21a504f52e5ee028aa416332f510b2e9cff5f722af":16:
"010001":MBEDTLS_MD_SHA1:"4046ca8baa3347ca27f49e0d81f9cc1d71be9ba517d4":"dd0f6cfe415e88e5a469a
51fbba6dfd40adb4384":"0630eebcd2856c24f798806e41f9e67345eda9ceda386acc9facaea1eeed06ace583709718d9d
169fadf414d5c76f92996833ef305b75b1e4b95f662a20faedc3bae0c4827a8bf8a88edbd57ec203a27a841f02e43a615b
ab1a8cac0701de34debdef62a088089b55ec36ea7522fd3ec8d06b6a073e6df833153bc0aefd93bd1a3":0

RSAES-OAEP Encryption Example
6_2
pkcs1_rsaes_oaep_encrypt:1029:16:"12b17f6dad2ecd19ff46dc13f7860f09e0e0cfb677b38a52592305ceaf022c166db
90d04ac29e33f7dd12d9faf66e0816bb63ead267cc7d46c17c37be214bca2a22d723a64e44407436b6fc965729aefc255
4f376cd5dcea68293780a62bf39d0029485a160bbb9e5dc0972d21a504f52e5ee028aa416332f510b2e9cff5f722af":16:
"010001":MBEDTLS_MD_SHA1:"5cc72c60231df03b3d40f9b57931bc31109f972527f28b19e7480c7288cb3c92b2
2512214e4be6c914792ddabdf57faa8aa7":"8d14bd946a1351148f5cae2ed9a0c653e85ebd85":"0ebc37376173a4fd2f8
9cc55c2ca62b26b11d51c3c7ce49e8845f74e7607317c436bc8d23b9667dfeb9d087234b47bc6837175ae5c0559f6b81
d7d22416d3e50f4ac533d8f0812f2db9e791fe9c775ac8b6ad0f535ad9ceb23a4a02014c58ab3f8d3161499a260f39348
e714ae2a1d3443208fd8b722ccfdfb393e98011f99e63f":0

RSAES-OAEP Encryption Example 6_3
pkcs1_rsaes_oaep_encrypt:1029:16:"12b17f6dad2ecd19ff46dc13f7860f09e0e0cfb677b38a52592305ceaf022c166db
90d04ac29e33f7dd12d9faf66e0816bb63ead267cc7d46c17c37be214bca2a22d723a64e44407436b6fc965729aefc255
4f376cd5dcea68293780a62bf39d0029485a160bbb9e5dc0972d21a504f52e5ee028aa416332f510b2e9cff5f722af":16:
"010001":MBEDTLS_MD_SHA1:"b20e651303092f4bccb43070c0f86d23049362ed96642fc5632c27db4a52e3d831
f2ab068b23b149879c002f6bf3feee97591112562c":"6c075bc45520f165c0bf5ea4c5df191bc9ef0e44":"0a98bf109361
9394436cf68d8f38e2f158fde8ea54f3435f239b8d06b8321844202476aeed96009492480ce3a8d705498c4c8c68f0150
1dc81db608f60087350c8c3b0bd2e9ef6a81458b7c801b89f2e4fe99d4900ba6a4b5e5a96d865dc676c7755928794130
d6280a8160a190f2df3ea7cf9aa0271d88e9e6905ecf1c5152d65":0

RSAES-OAEP
Encryption Example 6_4
pkcs1_rsaes_oaep_encrypt:1029:16:"12b17f6dad2ecd19ff46dc13f7860f09e0e0cfb677b38a52592305ceaf022c166db
90d04ac29e33f7dd12d9faf66e0816bb63ead267cc7d46c17c37be214bca2a22d723a64e44407436b6fc965729aefc255
4f376cd5dcea68293780a62bf39d0029485a160bbb9e5dc0972d21a504f52e5ee028aa416332f510b2e9cff5f722af":16:
"010001":MBEDTLS_MD_SHA1:"684e3038c5c041f7":"3bbc3bd6637dfe12846901029bf5b0c07103439c":"008e7a
67cacfb5c4e24bec7dee149117f19598ce8c45808fef88c608ff9cd6e695263b9a3c0ad4b8ba4c95238e96a8422b853562
9c8d5382374479ad13fa39974b242f9a759eeaf9c83ad5a8ca18940a0162ba755876df263f4bd50c6525c56090267c1f0
e09ce0899a0cf359e88120abd9bf893445b3cae77d3607359ae9a52f8":0

RSAES-OAEP

Encryption Example 6_5

pkcs1_rsaes_oaep_encrypt:1029:16:"12b17f6dad2ecd19ff46dc13f7860f09e0e0cfb677b38a52592305ceaf022c166db90d04ac29e33f7dd12d9faf66e0816bb63ead267cc7d46c17c37be214bca2a22d723a64e44407436b6fc965729aefc2554f376cd5dcea68293780a62bf39d0029485a160bbb9e5dc0972d21a504f52e5ee028aa416332f510b2e9cff5f722af":16:"010001":MBEDTLS_MD_SHA1:"32488cb262d041d6e4dd35f987bf3ca696db1f06ac29a44693":"b46b41893e8bef326f6759383a83071dae7fcabc":"00003474416c7b68bdf961c385737944d7f1f40cb395343c693cc0b4fe63b31fedf1eaeeac9ccc0678b31dc32e0977489514c4f09085f6298a9653f01aea4045ff582ee887be26ae575b73eef7f3774921e375a3d19adda0ca31aa1849887c1f42cac9677f7a2f4e923f6e5a868b38c084ef187594dc9f7f048fea2e02955384ab":0

RSAES-OAEP Encryption Example 6_6

pkcs1_rsaes_oaep_encrypt:1029:16:"12b17f6dad2ecd19ff46dc13f7860f09e0e0cfb677b38a52592305ceaf022c166db90d04ac29e33f7dd12d9faf66e0816bb63ead267cc7d46c17c37be214bca2a22d723a64e44407436b6fc965729aefc2554f376cd5dcea68293780a62bf39d0029485a160bbb9e5dc0972d21a504f52e5ee028aa416332f510b2e9cff5f722af":16:"010001":MBEDTLS_MD_SHA1:"50ba14be8462720279c306ba":"0a2403312a41e3d52f060fbc13a67de5cf7609a7":"0a026dda5fc8785f7bd9bf75327b63e85e2c0fdee5dadb65ebdcac9ae1de95c92c672ab433aa7a8e69ce6a6d8897fac4ac4a54de841ae5e5bbce7687879d79634cea7a30684065c714d52409b928256bbf53eabcd5231eb7259504537399bd29164b726d33a46da701360a4168a091ccab72d44a62fed246c0ffea5b1348ab5470":0

RSAES-OAEP

Encryption Example 7_1

pkcs1_rsaes_oaep_encrypt:1030:16:"311179f0bcfc9b9d3ca315d00ef30d7bdd3a2cfae9911bfedcb948b3a4782d0732b6ab44aa4bf03741a644dc01bec3e69b01a033e675d8acd7c4925c6b1aec3119051dfd89762d215d45475ffcb59f908148623f37177156f6ae86dd7a7c5f43dc1e1f908254058a284a5f06c0021793a87f1ac5feff7dcaee69c5e51a3789e373":16:"010001":MBEDTLS_MD_SHA1:"47aae909":"43dd09a07ff4cac71caa4632ee5e1c1daee4cd8f":"1688e4ce7794bba6cb7014169ecd559cede2a30b56a52b68d9fe18cf1973ef97b2a03153951c755f6294aa49adbdb55845ab6875fb3986c93ecf927962840d282f9e54ce8b690f7c0cb8bbd73440d9571d1b16cd9260f9eab4783cc482e5223dc60973871783ec27b0ae0fd47732cbc286a173fc92b00fb4ba6824647cd93c85c1":0

RSAES-OAEP

Encryption Example 7_2

pkcs1_rsaes_oaep_encrypt:1030:16:"311179f0bcfc9b9d3ca315d00ef30d7bdd3a2cfae9911bfedcb948b3a4782d0732b6ab44aa4bf03741a644dc01bec3e69b01a033e675d8acd7c4925c6b1aec3119051dfd89762d215d45475ffcb59f908148623f37177156f6ae86dd7a7c5f43dc1e1f908254058a284a5f06c0021793a87f1ac5feff7dcaee69c5e51a3789e373":16:"010001":MBEDTLS_MD_SHA1:"1d9b2e2223d9bc13bfb9f162ce735db48ba7c68f6822a0a1a7b6ae165834e7":"3a9c3cec7b84f9bd3adecbc673ec99d54b22bc9b":"1052ed397b2e01e1d0ee1c50bf24363f95e504f4a03434a08fd822574ed6b9736edbb5f390db10321479a8a139350e2bd4977c3778ef331f3e78ae118b268451f20a2f01d471f5d53c566937171b2dbc2d4bde459a5799f0372d6574239b2323d245d0bb81c286b63c89a361017337e4902f88a467f4c7f244bfd5ab46437ff3b6":0

RSAES-OAEP

Encryption Example 7_3

pkcs1_rsaes_oaep_encrypt:1030:16:"311179f0bcfc9b9d3ca315d00ef30d7bdd3a2cfae9911bfedcb948b3a4782d0732b6ab44aa4bf03741a644dc01bec3e69b01a033e675d8acd7c4925c6b1aec3119051dfd89762d215d45475ffcb59f908148623f37177156f6ae86dd7a7c5f43dc1e1f908254058a284a5f06c0021793a87f1ac5feff7dcaee69c5e51a3789e373":16:"010001":MBEDTLS_MD_SHA1:"d976fc":"76a75e5b6157a556cf8884bb2e45c293dd545cf5":"2155cd843ff24a4ee8badb7694260028a490813ba8b369a4cbf106ec148e5298707f5965be7d101c1049ea8584c24cd63455ad9c104d686282d3fb803a4c11c1c2e9b91c7178801d1b6640f003f5728df007b8a4ccc92bce05e41a27278d7c85018c52414313a5077789001d4f01910b72aad05d220aa14a58733a7489bc54556b":0

RSAES-OAEP Encryption Example 7_4
pkcs1_rsaes_oaep_encrypt:1030:16:"311179f0bcfc9b9d3ca315d00ef30d7bdd3a2cfae9911bfedcb948b3a4782d0732
b6ab44aa4bf03741a644dc01bec3e69b01a033e675d8acd7c4925c6b1aec3119051dfd89762d215d45475ffcb59f90814
8623f37177156f6ae86dd7a7c5f43dc1e1f908254058a284a5f06c0021793a87f1ac5feff7dcaee69c5e51a3789e373":16:
"010001":MBEDTLS_MD_SHA1:"d4738623df223aa43843df8467534c41d013e0c803c624e263666b239bde40a5f2
9aeb8de79e3daa61dd0370f49bd4b013834b98212aef6b1c5ee373b3cb":"7866314a6ad6f2b250a35941db28f5864b58
5859":"0ab14c373aeb7d4328d0aaad8c094d88b9eb098b95f21054a29082522be7c27a312878b637917e3d819e6c3c5
68db5d843802b06d51d9e98a2be0bf40c031423b00edfbff8320efb9171bd2044653a4cb9c5122f6c65e83cda2ec3c126
027a9c1a56ba874d0fea23f380b82cf240b8cf540004758c4c77d934157a74f3fc12bfac":0

RSAES-OAEP
Encryption Example 7_5
pkcs1_rsaes_oaep_encrypt:1030:16:"311179f0bcfc9b9d3ca315d00ef30d7bdd3a2cfae9911bfedcb948b3a4782d0732
b6ab44aa4bf03741a644dc01bec3e69b01a033e675d8acd7c4925c6b1aec3119051dfd89762d215d45475ffcb59f90814
8623f37177156f6ae86dd7a7c5f43dc1e1f908254058a284a5f06c0021793a87f1ac5feff7dcaee69c5e51a3789e373":16:
"010001":MBEDTLS_MD_SHA1:"bb47231ca5ea1d3ad46c99345d9a8a61":"b2166ed472d58db10cab2c6b000cccf1
0a7dc509":"028387a318277434798b4d97f460068df5298faba5041ba11761a1cb7316b24184114ec500257e2589ed3
b607a1ebbe97a6cc2e02bf1b681f42312a33b7a77d8e7855c4a6de03e3c04643f786b91a264a0d6805e2cea91e68177eb
7a64d9255e4f27e713b7ccec00dc200ebd21c2ea2bb890feae4942df941dc3f97890ed347478":0

RSAES-OAEP
Encryption Example 7_6
pkcs1_rsaes_oaep_encrypt:1030:16:"311179f0bcfc9b9d3ca315d00ef30d7bdd3a2cfae9911bfedcb948b3a4782d0732
b6ab44aa4bf03741a644dc01bec3e69b01a033e675d8acd7c4925c6b1aec3119051dfd89762d215d45475ffcb59f90814
8623f37177156f6ae86dd7a7c5f43dc1e1f908254058a284a5f06c0021793a87f1ac5feff7dcaee69c5e51a3789e373":16:
"010001":MBEDTLS_MD_SHA1:"2184827095d35c3f86f600e8e59754013296":"52673bde2ca166c2aa46131ac1dc
808d67d7d3b1":"14c678a94ad60525ef39e959b2f3ba5c097a94ff912b67dbace80535c187abd47d075420b1872152bb
a08f7fc31f313bbf9273c912fc4c0149a9b0cfb79807e346eb332069611bec0ff9bcd168f1f7c33e77313cea454b94e254
9eecf002e2acf7f6f2d2845d4fe0aab2e5a92ddf68c480ae11247935d1f62574842216ae674115":0

RSAES-OAEP Encryption Example 8_1
pkcs1_rsaes_oaep_encrypt:1031:16:"5bdf0e30d321dda5147f882408fa69195480df8f80d3f6e8bf5818504f36427ca9b
1f5540b9c65a8f6974cf8447a244d9280201bb49fcbbe6378d1944cd227e230f96e3d10f819dcef276c64a00b2a4b6701
e7d01de5fabde3b1e9a0df82f4631359cd22669647fbb1717246134ed7b497cfffbdc42b59c73a96ed90166212dff7":16:
"010001":MBEDTLS_MD_SHA1:"050b755e5e6880f7b9e9d692a74c37aae449b31bfea6deff83747a897f6c2c825bb
1adbf850a3c96994b5de5b33cbc7d4a17913a7967":"7706ffca1ecfb1ebee2a55e5c6e24cd2797a4125":"09b3683d8a2e
b0fb295b62ed1fb9290b714457b7825319f4647872af889b30409472020ad12912bf19b11d4819f49614824ffd84d09c
0a17e7d17309d12919790410aa2995699f6a86dbe3242b5acc23af45691080d6b1ae810fb3e3057087f0970092ce00be
9562ff4053b6262ce0caa93e13723d2e3a5ba075d45f0d61b54b61":0

RSAES-OAEP
Encryption Example 8_2
pkcs1_rsaes_oaep_encrypt:1031:16:"5bdf0e30d321dda5147f882408fa69195480df8f80d3f6e8bf5818504f36427ca9b
1f5540b9c65a8f6974cf8447a244d9280201bb49fcbbe6378d1944cd227e230f96e3d10f819dcef276c64a00b2a4b6701
e7d01de5fabde3b1e9a0df82f4631359cd22669647fbb1717246134ed7b497cfffbdc42b59c73a96ed90166212dff7":16:
"010001":MBEDTLS_MD_SHA1:"4eb68dcd93ca9b19df111bd43608f557026fe4aa1d5cfac227a3eb5ab9548c18a06
dded23f81825986b2fcd71109ecef7eff88873f075c2aa0c469f69c92bc":"a3717da143b4dcffbc742665a8fa950585548

343":"2ecf15c97c5a15b1476ae986b371b57a24284f4a162a8d0c8182e7905e792256f1812ba5f83f1f7a130e42dcc022
32844edc14a31a68ee97ae564a383a3411656424c5f62ddb646093c367be1fcda426cf00a06d8acb7e57776fbbd855ac3
df506fc16b1d7c3f2110f3d8068e91e186363831c8409680d8da9ecd8cf1fa20ee39d":0

RSAES-OAEP
Encryption Example 8_3
pkcs1_rsaes_oaep_encrypt:1031:16:"5bdf0e30d321dda5147f882408fa69195480df8f80d3f6e8bf5818504f36427ca9b
1f5540b9c65a8f6974cf8447a244d9280201bb49fcbbe6378d1944cd227e230f96e3d10f819dcef276c64a00b2a4b6701
e7d01de5fabde3b1e9a0df82f4631359cd22669647fbb1717246134ed7b497cfffbdc42b59c73a96ed90166212dff7":16:
"010001":MBEDTLS_MD_SHA1:"8604ac56328c1ab5ad917861":"ee06209073cca026bb264e5185bf8c68b7739f86
":"4bc89130a5b2dabb7c2fcf90eb5d0eaf9e681b7146a38f3173a3d9cfec52ea9e0a41932e648a9d69344c50da763f51a
03c95762131e8052254dcd2248cba40fd31667786ce05a2b7b531ac9dac9ed584a59b677c1a8aed8c5d15d68c05569e2
be780bf7db638fd2bfd2a85ab276860f3777338fca989ffd743d13ee08e0ca9893f":0

RSAES-OAEP
Encryption Example 8_4
pkcs1_rsaes_oaep_encrypt:1031:16:"5bdf0e30d321dda5147f882408fa69195480df8f80d3f6e8bf5818504f36427ca9b
1f5540b9c65a8f6974cf8447a244d9280201bb49fcbbe6378d1944cd227e230f96e3d10f819dcef276c64a00b2a4b6701
e7d01de5fabde3b1e9a0df82f4631359cd22669647fbb1717246134ed7b497cfffbdc42b59c73a96ed90166212dff7":16:
"010001":MBEDTLS_MD_SHA1:"fdda5fbf6ec361a9d9a4ac68af216a0686f438b1e0e5c36b955f74e107f39c0dddcc
":"990ad573dc48a973235b6d82543618f2e955105d":"2e456847d8fc36ff0147d6993594b9397227d577752c79d0f90
4fcb039d4d812fea605a7b574dd82ca786f93752348438ee9f5b5454985d5f0e1699e3e7ad175a32e15f03deb042ab9fe
1dd9db1bb86f8c089ccb45e7ef0c5ee7ca9b7290ca6b15bed47039788a8a93ff83e0e8d6244c71006362deef69b6f416fb
3c684383fbd0":0

RSAES-OAEP Encryption Example 8_5
pkcs1_rsaes_oaep_encrypt:1031:16:"5bdf0e30d321dda5147f882408fa69195480df8f80d3f6e8bf5818504f36427ca9b
1f5540b9c65a8f6974cf8447a244d9280201bb49fcbbe6378d1944cd227e230f96e3d10f819dcef276c64a00b2a4b6701
e7d01de5fabde3b1e9a0df82f4631359cd22669647fbb1717246134ed7b497cfffbdc42b59c73a96ed90166212dff7":16:
"010001":MBEDTLS_MD_SHA1:"4a5f4914bee25de3c69341de07":"ecc63b28f0756f22f52ac8e6ec1251a6ec30471
8":"1fb9356fd5c4b1796db2ebf7d0d393cc810adf6145defc2fce714f79d93800d5e2ac211ea8bbecca4b654b94c3b18b
30dd576ce34dc95436ef57a09415645923359a5d7b4171ef22c24670f1b229d3603e91f76671b7df97e7317c97734476
d5f3d17d21cf82b5ba9f83df2e588d36984fd1b584468bd23b2e875f32f68953f7b2":0

RSAES-OAEP
Encryption Example 8_6
pkcs1_rsaes_oaep_encrypt:1031:16:"5bdf0e30d321dda5147f882408fa69195480df8f80d3f6e8bf5818504f36427ca9b
1f5540b9c65a8f6974cf8447a244d9280201bb49fcbbe6378d1944cd227e230f96e3d10f819dcef276c64a00b2a4b6701
e7d01de5fabde3b1e9a0df82f4631359cd22669647fbb1717246134ed7b497cfffbdc42b59c73a96ed90166212dff7":16:
"010001":MBEDTLS_MD_SHA1:"8e07d66f7b880a72563abcd3f35092bc33409fb7f88f2472be":"3925c71b362d40
a0a6de42145579ba1e7dd459fc":"3afd9c6600147b21798d818c655a0f4c9212db26d0b0dfdc2a7594ccb3d22f5bf1d7c
3e112cd73fc7d509c7a8bafdd3c274d1399009f9609ec4be6477e453f075aa33db382870c1c3409aef392d7386ae3a696
b99a94b4da0589447e955d16c98b17602a59bd736279fcd8fb280c4462d590bfa9bf13fed570eafde97330a2c210":0

RSAES-OAEP
Encryption Example 9_1
pkcs1_rsaes_oaep_encrypt:1536:16:"cf2cd41e34ca3a728ea5cb8aff64c36d27bdef5364e336fd68d3123c5a196a8c287
013e853d5156d58d151954520fb4f6d7b17abb6817765909c576119659d902b1906ed8a2b10c155c24d124528dab9ee

ae379beac66e4a411786dcb8fd0062ebc030de1219a04c2a8c1b7dd3131e4d6b6caee2e31a5ed41ac1509b2ef1ee2ab18
364be568ca941c25ecc84ff9d643b5ec1aaae102a20d73f479b780fd6da91075212d9eac03a0674d899eba2e431f4c44b
615b6ba2232bd4b33baed73d625d":16:"010001":MBEDTLS_MD_SHA1:"f735fd55ba92592c3b52b8f9c4f69aaa1cb
ef8fe88add095595412467f9cf4ec0b896c59eda16210e7549c8abb10cdbc21a12ec9b6b5b8fd2f10399eb6":"8ec965f1
34a3ec9931e92a1ca0dc8169d5ea705c":"267bcd118acab1fc8ba81c85d73003cb8610fa55c1d97da8d48a7c7f06896a4
db751aa284255b9d36ad65f37653d829f1b37f97b8001942545b2fc2c55a7376ca7a1be4b1760c8e05a33e5aa2526b8d
98e317088e7834c755b2a59b12631a182c05d5d43ab1779264f8456f515ce57dfdf512d5493dab7b7338dc4b7d78db9c
091ac3baf537a69fc7f549d979f0eff9a94fda4169bd4d1d19a69c99e33c3b55490d501b39b1edae118ff6793a15326158
4d3a5f39f6e682e3d17c8cd1261fa72":0

RSAES-OAEP

Encryption Example 9_2

pkcs1_rsaes_oaep_encrypt:1536:16:"cf2cd41e34ca3a728ea5cb8aff64c36d27bdef5364e336fd68d3123c5a196a8c287
013e853d5156d58d151954520fb4f6d7b17abb6817765909c576119659d902b1906ed8a2b10c155c24d124528dab9ee
ae379beac66e4a411786dcb8fd0062ebc030de1219a04c2a8c1b7dd3131e4d6b6caee2e31a5ed41ac1509b2ef1ee2ab18
364be568ca941c25ecc84ff9d643b5ec1aaae102a20d73f479b780fd6da91075212d9eac03a0674d899eba2e431f4c44b
615b6ba2232bd4b33baed73d625d":16:"010001":MBEDTLS_MD_SHA1:"81b906605015a63aabe42ddf11e197891
2f5404c7474b26dce3ed482bf961ecc818bf420c54659":"ecb1b8b25fa50cdab08e56042867f4af5826d16c":"93ac9f06
71ec29acbb444effc1a5741351d60fdb0e393fbf754acf0de49761a14841df7772e9bc82773966a1584c4d72baea00118f
83f35cca6e537cbd4d811f5583b29783d8a6d94cd31be70d6f526c10ff09c6fa7ce069795a3fcd0511fd5fcb564bcc80ea
9c78f38b80012539d8a4ddf6fe81e9cddb7f50dbbbbcc7e5d86097ccf4ec49189fb8bf318be6d5a0715d516b49af19125
8cd32dc833ce6eb4673c03a19bbace88cc54895f636cc0c1ec89096d11ce235a265ca1764232a689ae8":0

RSAES-OAEP

Encryption Example 9_3

pkcs1_rsaes_oaep_encrypt:1536:16:"cf2cd41e34ca3a728ea5cb8aff64c36d27bdef5364e336fd68d3123c5a196a8c287
013e853d5156d58d151954520fb4f6d7b17abb6817765909c576119659d902b1906ed8a2b10c155c24d124528dab9ee
ae379beac66e4a411786dcb8fd0062ebc030de1219a04c2a8c1b7dd3131e4d6b6caee2e31a5ed41ac1509b2ef1ee2ab18
364be568ca941c25ecc84ff9d643b5ec1aaae102a20d73f479b780fd6da91075212d9eac03a0674d899eba2e431f4c44b
615b6ba2232bd4b33baed73d625d":16:"010001":MBEDTLS_MD_SHA1:"fd326429df9b890e09b54b18b8f34f1e24
":"e89bb032c6ce622cbdb53bc9466014ea77f777c0":"81ebdd95054b0c822ef9ad7693f5a87adfb4b4c4ce70df2df84ed
49c04da58ba5fc20a19e1a6e8b7a3900b22796dc4e869ee6b42792d15a8eceb56c09c69914e813cea8f6931e4b8ed6f42
1af298d595c97f4789c7caa612c7ef360984c21b93edc5401068b5af4c78a8771b984d53b8ea8adf2f6a7d4a0ba76c75e1
dd9f658f20ded4a46071d46d7791b56803d8fea7f0b0f8e41ae3f09383a6f9585fe7753eaaffd2bf94563108beecc207bbb
535f5fcc705f0dde9f708c62f49a9c90371d3":0

RSAES-OAEP

Encryption Example 9_4

pkcs1_rsaes_oaep_encrypt:1536:16:"cf2cd41e34ca3a728ea5cb8aff64c36d27bdef5364e336fd68d3123c5a196a8c287
013e853d5156d58d151954520fb4f6d7b17abb6817765909c576119659d902b1906ed8a2b10c155c24d124528dab9ee
ae379beac66e4a411786dcb8fd0062ebc030de1219a04c2a8c1b7dd3131e4d6b6caee2e31a5ed41ac1509b2ef1ee2ab18
364be568ca941c25ecc84ff9d643b5ec1aaae102a20d73f479b780fd6da91075212d9eac03a0674d899eba2e431f4c44b
615b6ba2232bd4b33baed73d625d":16:"010001":MBEDTLS_MD_SHA1:"f1459b5f0c92f01a0f723a2e5662484d8f8
c0a20fc29dad6acd43bb5f3effdf4e1b63e07fdfe6628d0d74ca19bf2d69e4a0abf86d293925a796772f8088e":"606f3b9
9c0b9ccd771eaa29ea0e4c884f3189ccc":"bcc35f94cde66cb1136625d625b94432a35b22f3d2fa11a613ff0fca5bd57f8
7b902ccdc1cd0aebcb0715ee869d1d1fe395f6793003f5eca465059c88660d446ff5f0818552022557e38c08a67ead991
262254f10682975ec56397768537f4977af6d5f6aaceb7fb25dec5937230231fd8978af49119a29f29e424ab8272b4756
2792d5c94f774b8829d0b0d9f1a8c9eddf37574d5fa248eefa9c5271fc5ec2579c81bdd61b410fa61fe36e424221c113ad

db275664c801d34ca8c6351e4a858":0

RSAES-OAEP
Encryption Example 9_5
pkcs1_rsaes_oaep_encrypt:1536:16:"cf2cd41e34ca3a728ea5cb8aff64c36d27bdef5364e336fd68d3123c5a196a8c287013e853d5156d58d151954520fb4f6d7b17abb6817765909c576119659d902b1906ed8a2b10c155c24d124528dab9eeae379beac66e4a411786dcb8fd0062ebc030de1219a04c2a8c1b7dd3131e4d6b6caee2e31a5ed41ac1509b2ef1ee2ab18364be568ca941c25ecc84ff9d643b5ec1aaae102a20d73f479b780fd6da91075212d9eac03a0674d899eba2e431f4c44b615b6ba2232bd4b33baed73d625d":16:"010001":MBEDTLS_MD_SHA1:"53e6e8c729d6f9c319dd317e74b0db8e4ccca25f3c8305746e137ac63a63ef3739e7b595abb96e8d55e54f7bd41ab433378ffb911d":"fcbc421402e9ecabc6082afa40ba5f26522c840e":"232afbc927fa08c2f6a27b87d4a5cb09c07dc26fae73d73a90558839f4fd66d281b87ec734bce237ba166698ed829106a7de6942cd6cdce78fed8d2e4d81428e66490d036264cef92af941d3e35055fe3981e14d29cbb9a4f67473063baec79a1179f5a17c9c1832f2838fd7d5e59bb9659d56dce8a019edef1bb3accc697cc6cc7a778f60a064c7f6f5d529c6210262e003de583e81e3167b89971fb8c0e15d44fffef89b53d8d64dd797d159b56d2b08ea5307ea12c241bd58d4ee278a1f2e":0

RSAES-OAEP
Encryption Example 9_6
pkcs1_rsaes_oaep_encrypt:1536:16:"cf2cd41e34ca3a728ea5cb8aff64c36d27bdef5364e336fd68d3123c5a196a8c287013e853d5156d58d151954520fb4f6d7b17abb6817765909c576119659d902b1906ed8a2b10c155c24d124528dab9eeae379beac66e4a411786dcb8fd0062ebc030de1219a04c2a8c1b7dd3131e4d6b6caee2e31a5ed41ac1509b2ef1ee2ab18364be568ca941c25ecc84ff9d643b5ec1aaae102a20d73f479b780fd6da91075212d9eac03a0674d899eba2e431f4c44b615b6ba2232bd4b33baed73d625d":16:"010001":MBEDTLS_MD_SHA1:"b6b28ea2198d0c1008bc64":"23aade0e1e08bb9b9a78d2302a52f9c21b2e1ba2":"438cc7dc08a68da249e42505f8573ba60e2c2773d5b290f4cf9dff718e842081c383e67024a0f29594ea987b9d25e4b738f285970d195abb3a8c8054e3d79d6b9c9a8327ba596f1259e27126674766907d8d582ff3a8476154929adb1e6d1235b2ccb4ec8f663ba9cc670a92bebd853c8dbf69c6436d016f61add836e94732450434207f9fd4c43dec2a12a958efa01efe2669899b5e604c255c55fb7166de5589e369597bb09168c06dd5db177e06a1740eb2d5c82faeca6d92fcee9931ba9f":0

RSAES-OAEP
Encryption Example 10_1
pkcs1_rsaes_oaep_encrypt:2048:16:"ae45ed5601cec6b8cc05f803935c674ddbe0d75c4c09fd7951fc6b0caec313a8df39970c518bffba5ed68f3f0d7f22a4029d413f1ae07e4ebe9e4177ce23e7f5404b569e4ee1bdcf3c1fb03ef113802d4f855eb9b5134b5a7c8085adcae6fa2fa1417ec3763be171b0c62b760ede23c12ad92b980884c641f5a8fac26bdad4a03381a22fe1b754885094c82506d4019a535a286afeb271bb9ba592de18dcf600c2aeeae56e02f7cf79fc14cf3bdc7cd84febbbf950ca90304b2219a7aa063aefa2c3c1980e560cd64afe779585b6107657b957857efde6010988ab7de417fc88d8f384c4e6e72c3f943e0c31c0c4a5cc36f879d8a3ac9d7d59860eaada6b83bb":16:"010001":MBEDTLS_MD_SHA1:"8bba6bf82a6c0f86d5f1756e97956870b08953b06b4eb205bc1694ee":"47e1ab7119fee56c95ee5eaad86f40d0aa63bd33":"53ea5dc08cd260fb3b858567287fa91552c30b2febfba213f0ae87702d068d19bab07fe574523dfb42139d68c3c5afeee0bfe4cb7969cbf382b804d6e61396144e2d0e60741f8993c3014b58b9b1957a8babcd23af854f4c356fb1662aa72bfcc7e586559dc4280d160c126785a723ebeebeff71f11594440aaef87d10793a8774a239d4a04c87fe1467b9daf85208ec6c7255794a96cc29142f9a8bd418e3c1fd67344b0cd0829df3b2bec60253196293c6b34d3f75d32f213dd45c6273d505adf4cced1057cb758fc26aeefa441255ed4e64c199ee075e7f16646182fdb464739b68ab5daff0e63e9552016824f054bf4d3c8c90a97bb6b6553284eb429fcc":0

RSAES-OAEP
Encryption Example 10_2
pkcs1_rsaes_oaep_encrypt:2048:16:"ae45ed5601cec6b8cc05f803935c674ddbe0d75c4c09fd7951fc6b0caec313a8df3

9970c518bffba5ed68f3f0d7f22a4029d413f1ae07e4ebe9e4177ce23e7f5404b569e4ee1bdcf3c1fb03ef113802d4f855e
b9b5134b5a7c8085adcae6fa2fa1417ec3763be171b0c62b760ede23c12ad92b980884c641f5a8fac26bdad4a03381a22
fe1b754885094c82506d4019a535a286afeb271bb9ba592de18dcf600c2aeeae56e02f7cf79fc14cf3bdc7cd84febbbf950
ca90304b2219a7aa063aefa2c3c1980e560cd64afe779585b6107657b957857efde6010988ab7de417fc88d8f384c4e6e
72c3f943e0c31c0c4a5cc36f879d8a3ac9d7d59860eaada6b83bb":16:"010001":MBEDTLS_MD_SHA1:"e6ad181f05
3b58a904f2457510373e57":"6d17f5b4c1ffac351d195bf7b09d09f09a4079cf":"a2b1a430a9d657e2fa1c2bb5ed43ffb2
5c05a308fe9093c01031795f5874400110828ae58fb9b581ce9dddd3e549ae04a0985459bde6c626594e7b05dc4278b2
a1465c1368408823c85e96dc66c3a30983c639664fc4569a37fe21e5a195b5776eed2df8d8d361af686e750229bbd663f
161868a50615e0c337bec0ca35fec0bb19c36eb2e0bbcc0582fa1d93aacdb061063f59f2ce1ee43605e5d89eca183d2acd
fe9f81011022ad3b43a3dd417dac94b4e11ea81b192966e966b182082e71964607b4f8002f36299844a11f2ae0faeac2e
ae70f8f4f98088acdcd0ac556e9fccc511521908fad26f04c64201450305778758b0538bf8b5bb144a828e629795":0

RSAES-OAEP

Encryption Example 10_3

pkcs1_rsaes_oaep_encrypt:2048:16:"ae45ed5601cec6b8cc05f803935c674ddbe0d75c4c09fd7951fc6b0caec313a8df3
9970c518bffba5ed68f3f0d7f22a4029d413f1ae07e4ebe9e4177ce23e7f5404b569e4ee1bdcf3c1fb03ef113802d4f855e
b9b5134b5a7c8085adcae6fa2fa1417ec3763be171b0c62b760ede23c12ad92b980884c641f5a8fac26bdad4a03381a22
fe1b754885094c82506d4019a535a286afeb271bb9ba592de18dcf600c2aeeae56e02f7cf79fc14cf3bdc7cd84febbbf950
ca90304b2219a7aa063aefa2c3c1980e560cd64afe779585b6107657b957857efde6010988ab7de417fc88d8f384c4e6e
72c3f943e0c31c0c4a5cc36f879d8a3ac9d7d59860eaada6b83bb":16:"010001":MBEDTLS_MD_SHA1:"510a2cf60e
866fa2340553c94ea39fbc256311e83e94454b4124":"385387514deccc7c740dd8cdf9daee49a1cbfd54":"9886c3e676
4a8b9a84e84148ebd8c3b1aa8050381a78f668714c16d9cfd2a6edc56979c535d9dee3b44b85c18be892899237171147
2216d95dda98d2ee8347c9b14dffdff84aa48d25ac06f7d7e65398ac967b1ce90925f67dce049b7f812db0742997a74d4
4fe81dbe0e7a3feaf2e5c40af888d550ddbbe3bc20657a29543f8fc2913b9bd1a61b2ab2256ec409bbd7dc0d17717ea25
c43f42ed27df8738bf4afc6766ff7aff0859555ee283920f4c8a63c4a7340cbafddc339ecdb4b0515002f96c932b5b79167
af699c0ad3fccfdf0f44e85a70262bf2e18fe34b850589975e867ff969d48eabf212271546cdc05a69ecb526e52870c836f
307bd798780ede":0

RSAES-OAEP

Encryption Example 10_4

pkcs1_rsaes_oaep_encrypt:2048:16:"ae45ed5601cec6b8cc05f803935c674ddbe0d75c4c09fd7951fc6b0caec313a8df3
9970c518bffba5ed68f3f0d7f22a4029d413f1ae07e4ebe9e4177ce23e7f5404b569e4ee1bdcf3c1fb03ef113802d4f855e
b9b5134b5a7c8085adcae6fa2fa1417ec3763be171b0c62b760ede23c12ad92b980884c641f5a8fac26bdad4a03381a22
fe1b754885094c82506d4019a535a286afeb271bb9ba592de18dcf600c2aeeae56e02f7cf79fc14cf3bdc7cd84febbbf950
ca90304b2219a7aa063aefa2c3c1980e560cd64afe779585b6107657b957857efde6010988ab7de417fc88d8f384c4e6e
72c3f943e0c31c0c4a5cc36f879d8a3ac9d7d59860eaada6b83bb":16:"010001":MBEDTLS_MD_SHA1:"bcdd190da3
b7d300df9a06e22caae2a75f10c91ff667b7c16bde8b53064a2649a94045c9":"5caca6a0f764161a9684f85d92b6e0ef37
ca8b65":"6318e9fb5c0d05e5307e1683436e903293ac4642358aaa223d7163013aba87e2dfda8e60c6860e29a1e92686
163ea0b9175f329ca3b131a1edd3a77759a8b97bad6a4f8f4396f28cf6f39ca58112e48160d6e203daa5856f3aca5ffed5
77af499408e3dfd233e3e604dbe34a9c4c9082de65527cac6331d29dc80e0508a0fa7122e7f329f6cca5cfa34d4d1da417
805457e008bec549e478ff9e12a763c477d15bbb78f5b69bd57830fc2c4ed686d79bc72a95d85f88134c6b0afe56a8ccf
bc855828bb339bd17909cf1d70de3335ae07039093e606d655365de6550b872cd6de1d440ee031b61945f629ad8a353
b0d40939e96a3c450d2a8d5eee9f678093c8":0

RSAES-OAEP

Encryption Example 10_5

pkcs1_rsaes_oaep_encrypt:2048:16:"ae45ed5601cec6b8cc05f803935c674ddbe0d75c4c09fd7951fc6b0caec313a8df3
9970c518bffba5ed68f3f0d7f22a4029d413f1ae07e4ebe9e4177ce23e7f5404b569e4ee1bdcf3c1fb03ef113802d4f855e

b9b5134b5a7c8085adcae6fa2fa1417ec3763be171b0c62b760ede23c12ad92b980884c641f5a8fac26bdad4a03381a22
fe1b754885094c82506d4019a535a286afeb271bb9ba592de18dcf600c2aeeae56e02f7cf79fc14cf3bdc7cd84febbbf950
ca90304b2219a7aa063aefa2c3c1980e560cd64afe779585b6107657b957857efde6010988ab7de417fc88d8f384c4e6e
72c3f943e0c31c0c4a5cc36f879d8a3ac9d7d59860eaada6b83bb":16:"010001":MBEDTLS_MD_SHA1:"a7dd6c7dc2
4b46f9dd5f1e91ada4c3b3df947e877232a9":"95bca9e3859894b3dd869fa7ecd5bbc6401bf3e4":"75290872ccfd4a450
5660d651f56da6daa09ca1301d890632f6a992f3d565cee464afded40ed3b5be9356714ea5aa7655f4a1366c2f17c728f6
f2c5a5d1f8e28429bc4e6f8f2cff8da8dc0e0a9808e45fd09ea2fa40cb2b6ce6ffff5c0e159d11b68d90a85f7b84e103b09e
682666480c657505c0929259468a314786d74eab131573cf234bf57db7d9e66cc6748192e002dc0deea930585f0831fd
cd9bc33d51f79ed2ffc16bcf4d59812fcebcaa3f9069b0e445686d644c25ccf63b456ee5fa6ffe96f19cdf751fed9eaf3595
7754dbf4bfea5216aa1844dc507cb2d080e722eba150308c2b5ff1193620f1766ecf4481bafb943bd292877f2136ca494a
ba0":0

RSAES-OAEP

Encryption Example 10_6

pkcs1_rsaes_oaep_encrypt:2048:16:"ae45ed5601cec6b8cc05f803935c674ddbe0d75c4c09fd7951fc6b0caec313a8df3
9970c518bffba5ed68f3f0d7f22a4029d413f1ae07e4ebe9e4177ce23e7f5404b569e4ee1bdcf3c1fb03ef113802d4f855e
b9b5134b5a7c8085adcae6fa2fa1417ec3763be171b0c62b760ede23c12ad92b980884c641f5a8fac26bdad4a03381a22
fe1b754885094c82506d4019a535a286afeb271bb9ba592de18dcf600c2aeeae56e02f7cf79fc14cf3bdc7cd84febbbf950
ca90304b2219a7aa063aefa2c3c1980e560cd64afe779585b6107657b957857efde6010988ab7de417fc88d8f384c4e6e
72c3f943e0c31c0c4a5cc36f879d8a3ac9d7d59860eaada6b83bb":16:"010001":MBEDTLS_MD_SHA1:"eaf1a73a1b
0c4609537de69cd9228bbcfb9a8ca8c6c3efaf056fe4a7f4634ed00b7c39ec6922d7b8ea2c04ebac":"9f47ddf42e97eea8
56a9bdbc714eb3ac22f6eb32":"2d207a73432a8fb4c03051b3f73b28a61764098dfa34c47a20995f8115aa6816679b55
7e82dbee584908c6e69782d7deb34dbd65af063d57fca76a5fd069492fd6068d9984d209350565a62e5c77f23038c12c
b10c6634709b547c46f6b4a709bd85ca122d74465ef97762c29763e06dbc7a9e738c78bfca0102dc5e79d65b973f2824
0caab2e161a78b57d262457ed8195d53e3c7ae9da021883c6db7c24afdd2322eac972ad3c354c5fcef1e146c3a0290fb6
7adf007066e00428d2cec18ce58f9328698defef4b2eb5ec76918fde1c198cbb38b7afc67626a9aefec4322bfd90d25634
81c9a221f78c8272c82d1b62ab914e1c69f6af6ef30ca5260db4a46":0

RSAES-OAEP

Decryption Test Vector Int

pkcs1_rsaes_oaep_decrypt:1024:16:"eecfae81b1b9b3c908810b10a1b5600199eb9f44aef4fda493b81a9e3d84f63212
4ef0236e5d1e3b7e28fae7aa040a2d5b252176459d1f397541ba2a58fb6599":16:"c97fb1f027f453f6341233eaaad1d93
53f6c42d08866b1d05a0f2035028b9d869840b41666b42e92ea0da3b43204b5cfce3352524d0416a5a441e700af46150
3":16:"bbf82f090682ce9c2338ac2b9da871f7368d07eed41043a440d6b6f07454f51fb8dfbaaf035c02ab61ea48ceeb6f
cd4876ed520d60e1ec4619719d8a5b8b807fafb8e0a3dfc737723ee6b4b7d93a2584ee6a649d060953748834b2454598
394ee0aab12d7b61a51f527a9a41f6c1687fe2537298ca2a8f5946f8e5fd091dbdcb":16:"11":MBEDTLS_MD_SHA1:"
d436e99569fd32a7c8a05bbc90d32c49":"aafd12f659cae63489b479e5076ddec2f06cb58f":"1253e04dc0a5397bb44a7
ab87e9bf2a039a33d1e996fc82a94ccd30074c95df763722017069e5268da5d1c0b4f872cf653c11df82314a67968dfeae
28def04bb6d84b1c31d654a1970e5783bd6eb96a024c2ca2f4a90fe9f2ef5c9c140e5bb48da9536ad8700c84fc9130adea
74e558d51a74ddf85d8b50de96838d6063e0955":0

RSAES-OAEP

Decryption Test Vector 1_1

pkcs1_rsaes_oaep_decrypt:1024:16:"d32737e7267ffe1341b2d5c0d150a81b586fb3132bed2f8d5262864a9cb9f30af3
8be448598d413a172efb802c21acf1c11c520c2f26a471dcad212eac7ca39d":16:"cc8853d1d54da630fac004f471f281c
7b8982d8224a490edbeb33d3e3d5cc93c4765703d1dd791642f1f116a0dd852be2419b2af72bfe9a030e860b0288b5d7
7":16:"a8b3b284af8eb50b387034a860f146c4919f318763cd6c5598c8ae4811a1e0abc4c7e0b082d693a5e7fced675cf
4668512772c0cbc64a742c6c630f533c8cc72f62ae833c40bf25842e984bb78bdbf97c0107d55bdb662f5c4e0fab9845c

b5148ef7392dd3aaff93ae1e6b667bb3d4247616d4f5ba10d4cfd226de88d39f16fb":16:"010001":MBEDTLS_MD_S
HA1:"6628194e12073db03ba94cda9ef9532397d50dba79b987004afefe34":"18b776ea21069d69776a33e96bad48e1
dda0a5ef":"354fe67b4a126d5d35fe36c777791a3f7ba13def484e2d3908aff722fad468fb21696de95d0be911c2d3174f
8afcc201035f7b6d8e69402de5451618c21a535fa9d7bfc5b8dd9fc243f8cf927db31322d6e881eaa91a996170e657a05a
266426d98c88003f8477c1227094a0d9fa1e8c4024309ce1ecccb5210035d47ac72e8a":0

RSAES-OAEP
Decryption Test Vector 1_2
pkcs1_rsaes_oaep_decrypt:1024:16:"d32737e7267ffe1341b2d5c0d150a81b586fb3132bed2f8d5262864a9cb9f30af3
8be448598d413a172efb802c21acf1c11c520c2f26a471dcad212eac7ca39d":16:"cc8853d1d54da630fac004f471f281c
7b8982d8224a490edbeb33d3e3d5cc93c4765703d1dd791642f1f116a0dd852be2419b2af72bfe9a030e860b0288b5d7
7":16:"a8b3b284af8eb50b387034a860f146c4919f318763cd6c5598c8ae4811a1e0abc4c7e0b082d693a5e7fced675cf
4668512772c0cbc64a742c6c630f533c8cc72f62ae833c40bf25842e984bb78bdbf97c0107d55bdb662f5c4e0fab9845c
b5148ef7392dd3aaff93ae1e6b667bb3d4247616d4f5ba10d4cfd226de88d39f16fb":16:"010001":MBEDTLS_MD_S
HA1:"750c4047f547e8e41411856523298ac9bae245efaf1397fbe56f9dd5":"0cc742ce4a9b7f32f951bcb251efd925fe4
fe35f":"640db1acc58e0568fe5407e5f9b701dff8c3c91e716c536fc7fcec6cb5b71c1165988d4a279e1577d730fc7a299
32e3f00c81515236d8d8e31017a7a09df4352d904cdeb79aa583adcc31ea698a4c05283daba9089be5491f67c1a4ee48d
c74bbbe6643aef846679b4cb395a352d5ed115912df696ffe0702932946d71492b44":0

RSAES-OAEP
Decryption Test Vector 1_3
pkcs1_rsaes_oaep_decrypt:1024:16:"d32737e7267ffe1341b2d5c0d150a81b586fb3132bed2f8d5262864a9cb9f30af3
8be448598d413a172efb802c21acf1c11c520c2f26a471dcad212eac7ca39d":16:"cc8853d1d54da630fac004f471f281c
7b8982d8224a490edbeb33d3e3d5cc93c4765703d1dd791642f1f116a0dd852be2419b2af72bfe9a030e860b0288b5d7
7":16:"a8b3b284af8eb50b387034a860f146c4919f318763cd6c5598c8ae4811a1e0abc4c7e0b082d693a5e7fced675cf
4668512772c0cbc64a742c6c630f533c8cc72f62ae833c40bf25842e984bb78bdbf97c0107d55bdb662f5c4e0fab9845c
b5148ef7392dd3aaff93ae1e6b667bb3d4247616d4f5ba10d4cfd226de88d39f16fb":16:"010001":MBEDTLS_MD_S
HA1:"d94ae0832e6445ce42331cb06d531a82b1db4baad30f746dc916df24d4e3c2451fff59a6423eb0e1d02d4fe646cf
699dfd818c6e97b051":"2514df4695755a67b288eaf4905c36eec66fd2fd":"423736ed035f6026af276c35c0b3741b365
e5f76ca091b4e8c29e2f0befee603595aa8322d602d2e625e95eb81b2f1c9724e822eca76db8618cf09c5343503a43608
35b5903bc637e3879fb05e0ef32685d5aec5067cd7cc96fe4b2670b6eac3066b1fcf5686b68589aafb7d629b02d8f8625
ca3833624d4800fb081b1cf94eb":0

RSAES-OAEP
Decryption Test Vector 1_4
pkcs1_rsaes_oaep_decrypt:1024:16:"d32737e7267ffe1341b2d5c0d150a81b586fb3132bed2f8d5262864a9cb9f30af3
8be448598d413a172efb802c21acf1c11c520c2f26a471dcad212eac7ca39d":16:"cc8853d1d54da630fac004f471f281c
7b8982d8224a490edbeb33d3e3d5cc93c4765703d1dd791642f1f116a0dd852be2419b2af72bfe9a030e860b0288b5d7
7":16:"a8b3b284af8eb50b387034a860f146c4919f318763cd6c5598c8ae4811a1e0abc4c7e0b082d693a5e7fced675cf
4668512772c0cbc64a742c6c630f533c8cc72f62ae833c40bf25842e984bb78bdbf97c0107d55bdb662f5c4e0fab9845c
b5148ef7392dd3aaff93ae1e6b667bb3d4247616d4f5ba10d4cfd226de88d39f16fb":16:"010001":MBEDTLS_MD_S
HA1:"52e650d98e7f2a048b4f86852153b97e01dd316f346a19f67a85":"c4435a3e1a18a68b6820436290a37cefb85db
3fb":"45ead4ca551e662c9800f1aca8283b0525e6abae30be4b4aba762fa40fd3d38e22abefc69794f6ebbbc05ddbb112
16247d2f412fd0fba87c6e3acd888813646fd0e48e785204f9c3f73d6d8239562722dddd8771fec48b83a31ee6f592c4cf
d4bc88174f3b13a112aae3b9f7b80e0fc6f7255ba880dc7d8021e22ad6a85f0755":0

RSAES-OAEP

Decryption Test Vector 1_5

pkcs1_rsaes_oaep_decrypt:1024:16:"d32737e7267ffe1341b2d5c0d150a81b586fb3132bed2f8d5262864a9cb9f30af38be448598d413a172efb802c21acf1c11c520c2f26a471dcad212eac7ca39d":16:"cc8853d1d54da630fac004f471f281c7b8982d8224a490edbeb33d3e3d5cc93c4765703d1dd791642f1f116a0dd852be2419b2af72bfe9a030e860b0288b5d77":16:"a8b3b284af8eb50b387034a860f146c4919f318763cd6c5598c8ae4811a1e0abc4c7e0b082d693a5e7fced675cf4668512772c0cbc64a742c6c630f533c8cc72f62ae833c40bf25842e984bb78bdbf97c0107d55bdb662f5c4e0fab9845cb5148ef7392dd3aaff93ae1e6b667bb3d4247616d4f5ba10d4cfd226de88d39f16fb":16:"010001":MBEDTLS_MD_SHA1:"8da89fd9e5f974a29feffb462b49180f6cf9e802":"b318c42df3be0f83fea823f5a7b47ed5e425a3b5":"36f6e34d94a8d34daacba33a2139d00ad85a9345a86051e73071620056b920e219005855a213a0f23897cdcd731b45257c777fe908202befdd0b58386b1244ea0cf539a05d5d10329da44e13030fd760dcd644cfef2094d1910d3f433e1c7c6dd18bc1f2df7f643d662fb9dd37ead9059190f4fa66ca39e869c4eb449cbdc439":0

RSAES-OAEP

Decryption Test Vector 1_6

pkcs1_rsaes_oaep_decrypt:1024:16:"d32737e7267ffe1341b2d5c0d150a81b586fb3132bed2f8d5262864a9cb9f30af38be448598d413a172efb802c21acf1c11c520c2f26a471dcad212eac7ca39d":16:"cc8853d1d54da630fac004f471f281c7b8982d8224a490edbeb33d3e3d5cc93c4765703d1dd791642f1f116a0dd852be2419b2af72bfe9a030e860b0288b5d77":16:"a8b3b284af8eb50b387034a860f146c4919f318763cd6c5598c8ae4811a1e0abc4c7e0b082d693a5e7fced675cf4668512772c0cbc64a742c6c630f533c8cc72f62ae833c40bf25842e984bb78bdbf97c0107d55bdb662f5c4e0fab9845cb5148ef7392dd3aaff93ae1e6b667bb3d4247616d4f5ba10d4cfd226de88d39f16fb":16:"010001":MBEDTLS_MD_SHA1:"26521050844271":"e4ec0982c2336f3a677f6a356174eb0ce887abc2":"42cee2617b1ecea4db3f4829386fbd61dafbf038e180d837c96366df24c097b4ab0fac6bdf590d821c9f10642e681ad05b8d78b378c0f46ce2fad63f74e0ad3df06b075d7eb5f5636f8d403b9059ca761b5c62bb52aa45002ea70baace08ded243b9d8cbd62a68ade265832b56564e43a6fa42ed199a099769742df1539e8255":0

RSAES-OAEP

Decryption Test Vector 2_1

pkcs1_rsaes_oaep_decrypt:1025:16:"0159dbde04a33ef06fb608b80b190f4d3e22bcc13ac8e4a081033abfa416edb0b338aa08b57309ea5a5240e7dc6e54378c69414c31d97ddb1f406db3769cc41a43":16:"012b652f30403b38b40995fd6ff41a1acc8ada70373236b7202d39b2ee30cfb46db09511f6f307cc61cc21606c18a75b8a62f822df031ba0df0dafd5506f568bd7":16:"01947c7fce90425f47279e70851f25d5e62316fe8a1df19371e3e628e260543e4901ef6081f68c0b8141190d2ae8daba7d1250ec6db636e944ec3722877c7c1d0a67f14b1694c5f0379451a43e49a32dde83670b73da91a1c99bc23b436a60055c610f0baf99c1a079565b95a3f1526632d1d4da60f20eda25e653c4f002766f45":16:"010001":MBEDTLS_MD_SHA1:"8ff00caa605c702830634d9a6c3d42c652b58cf1d92fec570beee7":"8c407b5ec2899e5099c53e8ce793bf94e71b1782":"0181af8922b9fcb4d79d92ebe19815992fc0c1439d8bcd491398a0f4ad3a329a5bd9385560db532683c8b7da04e4b12aed6aacdf471c34c9cda891addcc2df3456653aa6382e9ae59b54455257eb099d562bbe10453f2b6d13c59c02e10f1f8abb5da0d0570932dacf2d0901db729d0fefcc054e70968ea540c81b04bcaefe720e":0

RSAES-OAEP

Decryption Test Vector 2_2

pkcs1_rsaes_oaep_decrypt:1025:16:"0159dbde04a33ef06fb608b80b190f4d3e22bcc13ac8e4a081033abfa416edb0b338aa08b57309ea5a5240e7dc6e54378c69414c31d97ddb1f406db3769cc41a43":16:"012b652f30403b38b40995fd6ff41a1acc8ada70373236b7202d39b2ee30cfb46db09511f6f307cc61cc21606c18a75b8a62f822df031ba0df0dafd5506f568bd7":16:"01947c7fce90425f47279e70851f25d5e62316fe8a1df19371e3e628e260543e4901ef6081f68c0b8141190d2ae8daba7d1250ec6db636e944ec3722877c7c1d0a67f14b1694c5f0379451a43e49a32dde83670b73da91a1c99bc23b436a60055c610f0baf99c1a079565b95a3f1526632d1d4da60f20eda25e653c4f002766f45":16:"010001":MBEDTLS_MD_SHA1:"2d":"b600cf3c2e506d7f16778c910d3a8b003eee61d5":"018759ff1df63b27924105623144 16a8aeaf2ac634b46f940ab82d64dbf165eee33011da749d4bab6e2fcd18129c9e49277d8453112b429a222a8471b070993998e7588

61c4d3f6d749d91c4290d332c7a4ab3f7ea35ff3a07d497c955ff0ffc95006b62c6d296810d9bfab024196c7934012c2df978ef299aba239940cba10245":0

RSAES-OAEP
Decryption Test Vector 2_3
pkcs1_rsaes_oaep_decrypt:1025:16:"0159dbde04a33ef06fb608b80b190f4d3e22bcc13ac8e4a081033abfa416edb0b338aa08b57309ea5a5240e7dc6e54378c69414c31d97ddb1f406db3769cc41a43":16:"012b652f30403b38b40995fd6ff41a1acc8ada70373236b7202d39b2ee30cfb46db09511f6f307cc61cc21606c18a75b8a62f822df031ba0df0dafd5506f568bd7":16:"01947c7fce90425f47279e70851f25d5e62316fe8a1df19371e3e628e260543e4901ef6081f68c0b8141190d2ae8daba7d1250ec6db636e944ec3722877c7c1d0a67f14b1694c5f0379451a43e49a32dde83670b73da91a1c99bc23b436a60055c610f0baf99c1a079565b95a3f1526632d1d4da60f20eda25e653c4f002766f45":16:"010001":MBEDTLS_MD_SHA1:"74fc88c51bc90f77af9d5e9a4a70133d4b4e0b34da3c37c7ef8e":"a73768aeeaa91f9d8c1ed6f9d2b63467f07ccae3":"018802bab04c60325e81c4962311f2be7c2adce93041a00719c88f957575f2c79f1b7bc8ced115c706b311c08a2d986ca3b6a9336b147c29c6f229409ddec651bd1fdd5a0b7f610c9937fdb4a3a762364b8b3206b4ea485fd098d08f63d4aa8bb2697d027b750c32d7f74eaf5180d2e9b66b17cb2fa55523bc280da10d14be2053":0

RSAES-OAEP
Decryption Test Vector 2_4
pkcs1_rsaes_oaep_decrypt:1025:16:"0159dbde04a33ef06fb608b80b190f4d3e22bcc13ac8e4a081033abfa416edb0b338aa08b57309ea5a5240e7dc6e54378c69414c31d97ddb1f406db3769cc41a43":16:"012b652f30403b38b40995fd6ff41a1acc8ada70373236b7202d39b2ee30cfb46db09511f6f307cc61cc21606c18a75b8a62f822df031ba0df0dafd5506f568bd7":16:"01947c7fce90425f47279e70851f25d5e62316fe8a1df19371e3e628e260543e4901ef6081f68c0b8141190d2ae8daba7d1250ec6db636e944ec3722877c7c1d0a67f14b1694c5f0379451a43e49a32dde83670b73da91a1c99bc23b436a60055c610f0baf99c1a079565b95a3f1526632d1d4da60f20eda25e653c4f002766f45":16:"010001":MBEDTLS_MD_SHA1:"a7eb2a5036931d27d4e891326d99692ffadda9bf7efd3e34e622c4adc085f721dfe885072c78a203b151739be540fa8c153a10f00a":"9a7b3b0e708bd96f8190ecab4fb9b2b3805a8156":"00a4578cbc176318a638fba7d01df15746af44d4f6cd96d7e7c495cbf425b09c649d32bf886da48fbaf989a2117187cafb1fb580317690e3ccd446920b7af82b31db5804d87d01514acbfa9156e782f867f6bed9449e0e9a2c09bcecc6aa087636965e34b3ec766f2fe2e43018a2fddeb140616a0e9d82e5331024ee0652fc7641":0

RSAES-OAEP
Decryption Test Vector 2_5
pkcs1_rsaes_oaep_decrypt:1025:16:"0159dbde04a33ef06fb608b80b190f4d3e22bcc13ac8e4a081033abfa416edb0b338aa08b57309ea5a5240e7dc6e54378c69414c31d97ddb1f406db3769cc41a43":16:"012b652f30403b38b40995fd6ff41a1acc8ada70373236b7202d39b2ee30cfb46db09511f6f307cc61cc21606c18a75b8a62f822df031ba0df0dafd5506f568bd7":16:"01947c7fce90425f47279e70851f25d5e62316fe8a1df19371e3e628e260543e4901ef6081f68c0b8141190d2ae8daba7d1250ec6db636e944ec3722877c7c1d0a67f14b1694c5f0379451a43e49a32dde83670b73da91a1c99bc23b436a60055c610f0baf99c1a079565b95a3f1526632d1d4da60f20eda25e653c4f002766f45":16:"010001":MBEDTLS_MD_SHA1:"2ef2b066f854c33f3bdcbb5994a435e73d6c6c":"eb3cebbc4adc16bb48e88c8aec0e34af7f427fd3":"00ebc5f5fda77cfdad3c83641a9025e77d72d8a6fb33a810f5950f8d74c73e8d931e8634d86ab1246256ae07b6005b71b7f2fb98351218331ce69b8ffbdc9da08bbc9c704f876deb9df9fc2ec065cad87f9090b07acc17aa7f997b27aca48806e897f771d95141fe4526d8a5301b678627efab707fd40fbebd6e792a25613e7aec":0

RSAES-OAEP
Decryption Test Vector 2_6
pkcs1_rsaes_oaep_decrypt:1025:16:"0159dbde04a33ef06fb608b80b190f4d3e22bcc13ac8e4a081033abfa416edb0b338aa08b57309ea5a5240e7dc6e54378c69414c31d97ddb1f406db3769cc41a43":16:"012b652f30403b38b40995fd6ff41a1acc8ada70373236b7202d39b2ee30cfb46db09511f6f307cc61cc21606c18a75b8a62f822df031ba0df0dafd5506f5

68bd7":16:"01947c7fce90425f47279e70851f25d5e62316fe8a1df19371e3e628e260543e4901ef6081f68c0b8141190
d2ae8daba7d1250ec6db636e944ec3722877c7c1d0a67f14b1694c5f0379451a43e49a32dde83670b73da91a1c99bc23
b436a60055c610f0baf99c1a079565b95a3f1526632d1d4da60f20eda25e653c4f002766f45":16:"010001":MBEDTLS
_MD_SHA1:"8a7fb344c8b6cb2cf2ef1f643f9a3218f6e19bba89c0":"4c45cf4d57c98e3d6d2095adc51c489eb50dff84
":"010839ec20c27b9052e55befb9b77e6fc26e9075d7a54378c646abdf51e445bd5715de81789f56f1803d9170764a9e
93cb78798694023ee7393ce04bc5d8f8c5a52c171d43837e3aca62f609eb0aa5ffb0960ef04198dd754f57f7fbe6abf765
cf118b4ca443b23b5aab266f952326ac4581100644325f8b721acd5d04ff14ef3a":0

RSAES-OAEP
Decryption Example 3_1
pkcs1_rsaes_oaep_decrypt:1026:16:"01bf01d216d73595cf0270c2beb78d40a0d8447d31da919a983f7eea781b77d85f
e371b3e9373e7b69217d3150a02d8958de7fad9d555160958b4454127e0e7eaf":16:"018d3399658166db3829816d7b
295416759e9c91987f5b2d8aecd63b04b48bd7b2fcf229bb7f8a6dc88ba13dd2e39ad55b6d1a06160708f9700be80b8fd
3744ce7":16:"02b58fec039a860700a4d7b6462f93e6cdd491161ddd74f4e810b40e3c1652006a5c277b2774c11305a4
cbab5a78efa57e17a86df7a3fa36fc4b1d2249f22ec7c2dd6a463232accea906d66ebe80b5704b10729da6f833234abb5e
fdd4a292cbfad33b4d33fa7a14b8c397b56e3acd21203428b77cdfa33a6da706b3d8b0fc43e9":16:"010001":MBEDTL
S_MD_SHA1:"087820b569e8fa8d":"8ced6b196290805790e909074015e6a20b0c4894":"026a0485d96aebd96b4382
085099b962e6a2bdec3d90c8db625e14372de85e2d5b7baab65c8faf91bb5504fb495afce5c988b3f6a52e20e1d6cbd35
66c5cd1f2b8318bb542cc0ea25c4aab9932afa20760eaddec784396a07ea0ef24d4e6f4d37e5052a7a31e146aa480a111
bbe926401307e00f410033842b6d82fe5ce4dfae80":0

RSAES-OAEP
Decryption Example 3_2
pkcs1_rsaes_oaep_decrypt:1026:16:"01bf01d216d73595cf0270c2beb78d40a0d8447d31da919a983f7eea781b77d85f
e371b3e9373e7b69217d3150a02d8958de7fad9d555160958b4454127e0e7eaf":16:"018d3399658166db3829816d7b
295416759e9c91987f5b2d8aecd63b04b48bd7b2fcf229bb7f8a6dc88ba13dd2e39ad55b6d1a06160708f9700be80b8fd
3744ce7":16:"02b58fec039a860700a4d7b6462f93e6cdd491161ddd74f4e810b40e3c1652006a5c277b2774c11305a4
cbab5a78efa57e17a86df7a3fa36fc4b1d2249f22ec7c2dd6a463232accea906d66ebe80b5704b10729da6f833234abb5e
fdd4a292cbfad33b4d33fa7a14b8c397b56e3acd21203428b77cdfa33a6da706b3d8b0fc43e9":16:"010001":MBEDTL
S_MD_SHA1:"4653acaf171960b01f52a7be63a3ab21dc368ec43b50d82ec3781e04":"b4291d6567550848cc156967c
809baab6ca507f0":"024db89c7802989be0783847863084941bf209d761987e38f97cb5f6f1bc88da72a50b73ebaf11c
879c4f95df37b850b8f65d7622e25b1b889e80fe80baca2069d6e0e1d829953fc459069de98ea9798b451e557e99abf8f
e3d9ccf9096ebbf3e5255d3b4e1c6d2ecadf067a359eea86405acd47d5e165517ccafd47d6dbee4bf5":0

RSAES-OAEP
Decryption Example 3_3
pkcs1_rsaes_oaep_decrypt:1026:16:"01bf01d216d73595cf0270c2beb78d40a0d8447d31da919a983f7eea781b77d85f
e371b3e9373e7b69217d3150a02d8958de7fad9d555160958b4454127e0e7eaf":16:"018d3399658166db3829816d7b
295416759e9c91987f5b2d8aecd63b04b48bd7b2fcf229bb7f8a6dc88ba13dd2e39ad55b6d1a06160708f9700be80b8fd
3744ce7":16:"02b58fec039a860700a4d7b6462f93e6cdd491161ddd74f4e810b40e3c1652006a5c277b2774c11305a4
cbab5a78efa57e17a86df7a3fa36fc4b1d2249f22ec7c2dd6a463232accea906d66ebe80b5704b10729da6f833234abb5e
fdd4a292cbfad33b4d33fa7a14b8c397b56e3acd21203428b77cdfa33a6da706b3d8b0fc43e9":16:"010001":MBEDTL
S_MD_SHA1:"d94cd0e08fa404ed89":"ce8928f6059558254008badd9794fadcd2fd1f65":"0239bce68103244152887
7d6d1c8bb28aa3bc97f1df5845636189957976838 44ca86664732f4bed7a0aab083aaabfb7238f582e30958c2024e44e5
7043b97950fd543da977c90cdde5337d618442f99e60d7783ab59ce6dd9d69c47ad1e962bec22d05895cff8d3f64ed52
61d92b26785103934849 90ba3f7f06818ae6ffce8a3a":0

RSAES-OAEP

Decryption Example 3_4

pkcs1_rsaes_oaep_decrypt:1026:16:"01bf01d216d73595cf0270c2beb78d40a0d8447d31da919a983f7eea781b77d85f
e371b3e9373e7b69217d3150a02d8958de7fad9d555160958b4454127e0e7eaf":16:"018d3399658166db3829816d7b
295416759e9c91987f5b2d8aecd63b04b48bd7b2fcf229bb7f8a6dc88ba13dd2e39ad55b6d1a06160708f9700be80b8fd
3744ce7":16:"02b58fec039a860700a4d7b6462f93e6cdd491161ddd74f4e810b40e3c1652006a5c277b2774c11305a4
cbab5a78efa57e17a86df7a3fa36fc4b1d2249f22ec7c2dd6a463232accea906d66ebe80b5704b10729da6f833234abb5e
fdd4a292cbfad33b4d33fa7a14b8c397b56e3acd21203428b77cdfa33a6da706b3d8b0fc43e9":16:"010001":MBEDTL
S_MD_SHA1:"6cc641b6b61e6f963974dad23a9013284ef1":"6e2979f52d6814a57d83b090054888f119a5b9a3":"02
994c62afd76f498ba1fd2cf642857fca81f4373cb08f1cbaee6f025c3b512b42c3e8779113476648039dbe0493f9246292
fac28950600e7c0f32edf9c81b9dec45c3bde0cc8d8847590169907b7dc5991ceb29bb0714d613d96df0f12ec5d8d3507
c8ee7ae78dd83f216fa61de100363aca48a7e914ae9f42ddfbe943b09d9a0":0

RSAES-OAEP

Decryption Example 3_5

pkcs1_rsaes_oaep_decrypt:1026:16:"01bf01d216d73595cf0270c2beb78d40a0d8447d31da919a983f7eea781b77d85f
e371b3e9373e7b69217d3150a02d8958de7fad9d555160958b4454127e0e7eaf":16:"018d3399658166db3829816d7b
295416759e9c91987f5b2d8aecd63b04b48bd7b2fcf229bb7f8a6dc88ba13dd2e39ad55b6d1a06160708f9700be80b8fd
3744ce7":16:"02b58fec039a860700a4d7b6462f93e6cdd491161ddd74f4e810b40e3c1652006a5c277b2774c11305a4
cbab5a78efa57e17a86df7a3fa36fc4b1d2249f22ec7c2dd6a463232accea906d66ebe80b5704b10729da6f833234abb5e
fdd4a292cbfad33b4d33fa7a14b8c397b56e3acd21203428b77cdfa33a6da706b3d8b0fc43e9":16:"010001":MBEDTL
S_MD_SHA1:"df5151832b61f4f25891fb4172f328d2eddf8371ffcfdbe997939295f30eca6918017cfda1153bf7a6af87
593223":"2d760bfe38c59de34cdc8b8c78a38e66284a2d27":"0162042ff6969592a6167031811a239834ce638abf54fe
c8b99478122afe2ee67f8c5b18b0339805bfdbc5a4e6720b37c59cfba942464c597ff532a119821545fd2e59b114e61daf
71820529f5029cf524954327c34ec5e6f5ba7efcc4de943ab8ad4ed787b1454329f70db798a3a8f4d92f8274e2b2948ad
e627ce8ee33e43c60":0

RSAES-OAEP

Decryption Example 3_6

pkcs1_rsaes_oaep_decrypt:1026:16:"01bf01d216d73595cf0270c2beb78d40a0d8447d31da919a983f7eea781b77d85f
e371b3e9373e7b69217d3150a02d8958de7fad9d555160958b4454127e0e7eaf":16:"018d3399658166db3829816d7b
295416759e9c91987f5b2d8aecd63b04b48bd7b2fcf229bb7f8a6dc88ba13dd2e39ad55b6d1a06160708f9700be80b8fd
3744ce7":16:"02b58fec039a860700a4d7b6462f93e6cdd491161ddd74f4e810b40e3c1652006a5c277b2774c11305a4
cbab5a78efa57e17a86df7a3fa36fc4b1d2249f22ec7c2dd6a463232accea906d66ebe80b5704b10729da6f833234abb5e
fdd4a292cbfad33b4d33fa7a14b8c397b56e3acd21203428b77cdfa33a6da706b3d8b0fc43e9":16:"010001":MBEDTL
S_MD_SHA1:"3c3bad893c544a6d520ab022319188c8d504b7a788b850903b85972eaa18552e1134a7ad6098826254
ff7ab672b3d8eb3158fac6d4cbaef1":"f174779c5fd3cfe007badcb7a36c9b55bfcfbf0e":"00112051e75d064943bc4478
075e43482fd59cee0679de6893eec3a943daa490b9691c93dfc0464b6623b9f3dbd3e70083264f034b374f74164e1a007
63725e574744ba0b9db83434f31df96f6e2a26f6d8eba348bd4686c2238ac07c37aac3785d1c7eea2f819fd91491798ed
8e9cef5e43b781b0e0276e37c43ff9492d005730":0

RSAES-OAEP

Decryption Example 4_1

pkcs1_rsaes_oaep_decrypt:1027:16:"027458c19ec1636919e736c9af25d609a51b8f561d19c6bf6943dd1ee1ab8a4a3f
232100bd40b88decc6ba235548b6ef792a11c9de823d0a7922c7095b6eba5701":16:"0210ee9b33ab61716e27d251bd
465f4b35a1a232e2da00901c294bf22350ce490d099f642b5375612db63ba1f20386492bf04d34b3c22bceb909d13441
b53b5139":16:"051240b6cc0004fa48d0134671c078c7c8dec3b3e2f25bc2564467339db38853d06b85eea5b2de353bf
f42ac2e46bc97fae6ac9618da9537a5c8f553c1e357625991d6108dcd7885fb3a25413f53efcad948cb35cd9b9ae9c1c67
626d113d57dde4c5bea76bb5bb7de96c00d07372e9685a6d75cf9d239fa148d70931b5f3fb039":16:"010001":MBED

TLS_MD_SHA1:"4a86609534ee434a6cbca3f7e962e76d455e3264c19f605f6e5ff6137c65c56d7fb344cd52bc93374f
3d166c9f0c6f9c506bad19330972d2":"1cac19ce993def55f98203f6852896c95ccca1f3":"04cce19614845e094152a3f
e18e54e3330c44e5efbc64ae16886cb1869014cc5781b1f8f9e045384d0112a135ca0d12e9c88a8e4063416deaae3844f
60d6e96fe155145f4525b9a34431ca3766180f70e15a5e5d8e8b1a516ff870609f13f896935ced188279a58ed13d07114
277d75c6568607e0ab092fd803a223e4a8ee0b1a8":0

RSAES-OAEP
Decryption Example 4_2
pkcs1_rsaes_oaep_decrypt:1027:16:"027458c19ec1636919e736c9af25d609a51b8f561d19c6bf6943dd1ee1ab8a4a3f
232100bd40b88decc6ba235548b6ef792a11c9de823d0a7922c7095b6eba5701":16:"0210ee9b33ab61716e27d251bd
465f4b35a1a232e2da00901c294bf22350ce490d099f642b5375612db63ba1f20386492bf04d34b3c22bceb909d13441
b53b5139":16:"051240b6cc0004fa48d0134671c078c7c8dec3b3e2f25bc2564467339db38853d06b85eea5b2de353bf
f42ac2e46bc97fae6ac9618da9537a5c8f553c1e357625991d6108dcd7885fb3a25413f53efcad948cb35cd9b9ae9c1c67
626d113d57dde4c5bea76bb5bb7de96c00d07372e9685a6d75cf9d239fa148d70931b5f3fb039":16:"010001":MBED
TLS_MD_SHA1:"b0adc4f3fe11da59ce992773d9059943c03046497ee9d9f9a06df1166db46d98f58d27ec074c02eee
6cbe2449c8b9fc5080c5c3f4433092512ec46aa793743c8":"f545d5897585e3db71aa0cb8da76c51d032ae963":"0097b
698c6165645b303486fbf5a2a4479c0ee85889b541a6f0b858d6b6597b13b854eb4f839af03399a80d79bda6578c841f
90d645715b280d37143992dd186c80b949b775cae97370e4ec97443136c6da484e970ffdb1323a20847821d3b18381d
e13bb49aaea66530c4a4b8271f3eae172cd366e07e6636f1019d2a28aed15e":0

RSAES-OAEP
Decryption Example 4_3
pkcs1_rsaes_oaep_decrypt:1027:16:"027458c19ec1636919e736c9af25d609a51b8f561d19c6bf6943dd1ee1ab8a4a3f
232100bd40b88decc6ba235548b6ef792a11c9de823d0a7922c7095b6eba5701":16:"0210ee9b33ab61716e27d251bd
465f4b35a1a232e2da00901c294bf22350ce490d099f642b5375612db63ba1f20386492bf04d34b3c22bceb909d13441
b53b5139":16:"051240b6cc0004fa48d0134671c078c7c8dec3b3e2f25bc2564467339db38853d06b85eea5b2de353bf
f42ac2e46bc97fae6ac9618da9537a5c8f553c1e357625991d6108dcd7885fb3a25413f53efcad948cb35cd9b9ae9c1c67
626d113d57dde4c5bea76bb5bb7de96c00d07372e9685a6d75cf9d239fa148d70931b5f3fb039":16:"010001":MBED
TLS_MD_SHA1:"bf6d42e701707b1d0206b0c8b45a1c72641ff12889219a82bdea965b5e79a96b0d0163ed9d578ec9
ada20f2fbcf1ea3c4089d83419ba81b0c60f3606da99":"ad997feef730d6ea7be60d0dc52e72eacbfdd275":"0301f935e9
c47abcb48acbbe09895d9f5971af14839da4ff95417ee453d1fd77319072bb7297e1b55d7561cd9d1bb24c1a9a37c6198
64308242804879d86ebd001dce5183975e1506989b70e5a83434154d5cbfd6a24787e60eb0c658d2ac193302d1192c6
e622d4a12ad4b53923bca246df31c6395e37702c6a78ae081fb9d065":0

RSAES-OAEP
Decryption Example 4_4
pkcs1_rsaes_oaep_decrypt:1027:16:"027458c19ec1636919e736c9af25d609a51b8f561d19c6bf6943dd1ee1ab8a4a3f
232100bd40b88decc6ba235548b6ef792a11c9de823d0a7922c7095b6eba5701":16:"0210ee9b33ab61716e27d251bd
465f4b35a1a232e2da00901c294bf22350ce490d099f642b5375612db63ba1f20386492bf04d34b3c22bceb909d13441
b53b5139":16:"051240b6cc0004fa48d0134671c078c7c8dec3b3e2f25bc2564467339db38853d06b85eea5b2de353bf
f42ac2e46bc97fae6ac9618da9537a5c8f553c1e357625991d6108dcd7885fb3a25413f53efcad948cb35cd9b9ae9c1c67
626d113d57dde4c5bea76bb5bb7de96c00d07372e9685a6d75cf9d239fa148d70931b5f3fb039":16:"010001":MBED
TLS_MD_SHA1:"fb2ef112f5e766eb94019297934794f7be2f6fc1c58e":"136454df5730f73c807a7e40d8c1a312ac5b
9dd3":"02d110ad30afb727beb691dd0cf17d0af1a1e7fa0cc040ec1a4ba26a42c59d0a796a2e22c8f357ccc98b6519ace
b682e945e62cb734614a529407cd452bee3e44fece8423cc19e55548b8b994b849c7ecde4933e76037e1d0ce44275b08
710c68e430130b929730ed77e09b015642c5593f04e4ffb9410798102a8e96ffdfe11e4":0

RSAES-OAEP

Decryption Example 4_5

pkcs1_rsaes_oaep_decrypt:1027:16:"027458c19ec1636919e736c9af25d609a51b8f561d19c6bf6943dd1ee1ab8a4a3f232100bd40b88decc6ba235548b6ef792a11c9de823d0a7922c7095b6eba5701":16:"0210ee9b33ab61716e27d251bd465f4b35a1a232e2da00901c294bf22350ce490d099f642b5375612db63ba1f20386492bf04d34b3c22bceb909d13441b53b5139":16:"051240b6cc0004fa48d0134671c078c7c8dec3b3e2f25bc2564467339db38853d06b85eea5b2de353bff42ac2e46bc97fae6ac9618da9537a5c8f553c1e357625991d6108dcd7885fb3a25413f53efcad948cb35cd9b9ae9c1c67626d113d57dde4c5bea76bb5bb7de96c00d07372e9685a6d75cf9d239fa148d70931b5f3fb039":16:"010001":MBEDTLS_MD_SHA1:"28ccd447bb9e85166dabb9e5b7d1adadc4b9d39f204e96d5e440ce9ad928bc1c2284":"bca8057f824b2ea257f2861407eef63d33208681":"00dbb8a7439d90efd919a377c54fae8fe11ec58c3b858362e23ad1b8a44310799066b99347aa525691d2adc58d9b06e34f288c170390c5f0e11c0aa3645959f18ee79e8f2be8d7ac5c23d061f18dd74b8c5f2a58fcb5eb0c54f99f01a8324756829253658334094 8d7a8c97c4acd1e98d1e29dc320e97a260532a8aa7a758a1ec2":0

RSAES-OAEP

Decryption Example 4_6

pkcs1_rsaes_oaep_decrypt:1027:16:"027458c19ec1636919e736c9af25d609a51b8f561d19c6bf6943dd1ee1ab8a4a3f232100bd40b88decc6ba235548b6ef792a11c9de823d0a7922c7095b6eba5701":16:"0210ee9b33ab61716e27d251bd465f4b35a1a232e2da00901c294bf22350ce490d099f642b5375612db63ba1f20386492bf04d34b3c22bceb909d13441b53b5139":16:"051240b6cc0004fa48d0134671c078c7c8dec3b3e2f25bc2564467339db38853d06b85eea5b2de353bff42ac2e46bc97fae6ac9618da9537a5c8f553c1e357625991d6108dcd7885fb3a25413f53efcad948cb35cd9b9ae9c1c67626d113d57dde4c5bea76bb5bb7de96c00d07372e9685a6d75cf9d239fa148d70931b5f3fb039":16:"010001":MBEDTLS_MD_SHA1:"f22242751ec6b1":"2e7e1e17f647b5ddd033e15472f90f6812f3ac4e":"00a5ffa4768c8bbecaee2db77e8f2eec99595933545520835e5ba7db9493d3e17cddefe6a5f567624471908db4e2d83a0fbee60608fc84049503b2234a07dc83b27b22847ad8920ff42f674ef79b76280b00233d2b51b8cb2703a9d42bfbc8250c96ec32c051e57f1b4ba528db89c37e4c54e27e6e64ac69635ae887d9541619a9":0

RSAES-OAEP

Decryption Example 5_1

pkcs1_rsaes_oaep_decrypt:1028:16:"03b0d3962f6d17549cbfca11294348dcf0e7e39f8c2bc6824f2164b606d687860dae1e632393cfedf513228229069e2f60e4acd7e633a436063f82385f48993707":16:"02e4c32e2f517269b7072309f00c0e31365f7ce28b236b82912df239abf39572cf0ed604b02982e53564c52d6a05397de5c052a2fddc141ef7189836346aeb331f":16:"0aadf3f9c125e5d891f31ac448e993defe580f802b45f9d7f22ba5021e9c47576b5a1e68031ba9db4e6dabe4d96a1d6f3d267268cff408005f118efcadb99888d1c234467166b2a2b849a05a889c060ac0da0c5fae8b55f309ba62e703742fa0326f2d10b011021489ff497770190d895fd39f52293c39efd73a698bdab9f10ed9":16:"010001":MBEDTLS_MD_SHA1:"af71a901e3a61d3132f0fc1fdb474f9ea6579257ffc24d164170145b3dbde8":"44c92e283f77b9499c603d963660c87d2f939461":"036046a4a47d9ed3ba9a89139c105038eb7492b05a5d68bfd53accff4597f7a68651b47b4a4627d927e485eed7b4566420e8b409879e5d606eae251d22a5df799f7920bfc117b992572a53b1263146bcea03385cc5e853c9a101c8c3e1bda31a519807496c6cb5e5efb408823a352b8fa0661fb664efadd593deb99fff5ed000e5":0

RSAES-OAEP

Decryption Example 5_2

pkcs1_rsaes_oaep_decrypt:1028:16:"03b0d3962f6d17549cbfca11294348dcf0e7e39f8c2bc6824f2164b606d687860dae1e632393cfedf513228229069e2f60e4acd7e633a436063f82385f48993707":16:"02e4c32e2f517269b7072309f00c0e31365f7ce28b236b82912df239abf39572cf0ed604b02982e53564c52d6a05397de5c052a2fddc141ef7189836346aeb331f":16:"0aadf3f9c125e5d891f31ac448e993defe580f802b45f9d7f22ba5021e9c47576b5a1e68031ba9db4e6dabe4d96a1d6f3d267268cff408005f118efcadb99888d1c234467166b2a2b849a05a889c060ac0da0c5fae8b55f309ba62e703742fa0326f2d10b011021489ff497770190d895fd39f52293c39efd73a698bdab9f10ed9":16:"010001":MBEDTLS_MD_SHA1:"a3b844a08239a8ac41605af17a6cfda4d350136585903a417a79268760519a4b4ac3303ec73f0f87cfb323

99":"cb28f5860659fceee49c3eeafce625a70803bd32":"03d6eb654edce615bc59f455265ed4e5a18223cbb9be4e4069b473804d5de96f54dcaaa603d049c5d94aa1470dfcd2254066b7c7b61ff1f6f6770e3215c51399fd4e34ec5082bc48f089840ad04354ae66dc0f1bd18e461a33cc1258b443a2837a6df26759aa2302334986f87380c9cc9d53be9f99605d2c9a97da7b0915a4a7ad":0

RSAES-OAEP

Decryption Example 5_3

pkcs1_rsaes_oaep_decrypt:1028:16:"03b0d3962f6d17549cbfca11294348dcf0e7e39f8c2bc6824f2164b606d687860dae1e632393cfedf513228229069e2f60e4acd7e633a436063f82385f48993707":16:"02e4c32e2f517269b7072309f00c0e31365f7ce28b236b82912df239abf39572cf0ed604b02982e53564c52d6a05397de5c052a2fddc141ef7189836346aeb331f":16:"0aadf3f9c125e5d891f31ac448e993defe580f802b45f9d7f22ba5021e9c47576b5a1e68031ba9db4e6dabe4d96a1d6f3d267268cff408005f118efcadb99888d1c234467166b2a2b849a05a889c060ac0da0c5fae8b55f309ba62e703742fa0326f2d10b011021489ff497770190d895fd39f52293c39efd73a698bdab9f10ed9":16:"010001":MBEDTLS_MD_SHA1:"308b0ecbd2c76cb77fc6f70c5edd233fd2f20929d629f026953bb62a8f4a3a314bde195de85b5f816da2aab074d26cb6acddf323ae3b9c678ac3cf12fbdde7":"2285f40d770482f9a9efa2c72cb3ac55716dc0ca":"0770952181649f9f9f07ff626ff3a22c35c462443d905d456a9fd0bff43cac2ca7a9f554e9478b9acc3ac838b02040ffd3e1847de2e4253929f9dd9ee4044325a9b05cabb808b2ee840d34e15d105a3f1f7b27695a1a07a2d73fe08ecaaa3c9c9d4d5a89ff890d54727d7ae40c0ec1a8dd86165d8ee2c6368141016a48b55b6967":0

RSAES-OAEP

Decryption Example 5_4

pkcs1_rsaes_oaep_decrypt:1028:16:"03b0d3962f6d17549cbfca11294348dcf0e7e39f8c2bc6824f2164b606d687860dae1e632393cfedf513228229069e2f60e4acd7e633a436063f82385f48993707":16:"02e4c32e2f517269b7072309f00c0e31365f7ce28b236b82912df239abf39572cf0ed604b02982e53564c52d6a05397de5c052a2fddc141ef7189836346aeb331f":16:"0aadf3f9c125e5d891f31ac448e993defe580f802b45f9d7f22ba5021e9c47576b5a1e68031ba9db4e6dabe4d96a1d6f3d267268cff408005f118efcadb99888d1c234467166b2a2b849a05a889c060ac0da0c5fae8b55f309ba62e703742fa0326f2d10b011021489ff497770190d895fd39f52293c39efd73a698bdab9f10ed9":16:"010001":MBEDTLS_MD_SHA1:"15c5b9ee1185":"49fa45d3a78dd10dfd577399d1eb00af7eed5513":"0812b76768ebcb642d040258e5f4441a018521bd96687e6c5e899fcd6c17588ff59a82cc8ae03a4b45b31299af1788c329f7dcd285f8cf4ced82606b97612671a45bedca133442144d1617d114f802857f0f9d739751c57a3f9ee400912c61e2e6992be031a43dd48fa6ba14eef7c422b5edc4e7afa04fdd38f402d1c8bb719abf":0

RSAES-OAEP

Decryption Example 5_5

pkcs1_rsaes_oaep_decrypt:1028:16:"03b0d3962f6d17549cbfca11294348dcf0e7e39f8c2bc6824f2164b606d687860dae1e632393cfedf513228229069e2f60e4acd7e633a436063f82385f48993707":16:"02e4c32e2f517269b7072309f00c0e31365f7ce28b236b82912df239abf39572cf0ed604b02982e53564c52d6a05397de5c052a2fddc141ef7189836346aeb331f":16:"0aadf3f9c125e5d891f31ac448e993defe580f802b45f9d7f22ba5021e9c47576b5a1e68031ba9db4e6dabe4d96a1d6f3d267268cff408005f118efcadb99888d1c234467166b2a2b849a05a889c060ac0da0c5fae8b55f309ba62e703742fa0326f2d10b011021489ff497770190d895fd39f52293c39efd73a698bdab9f10ed9":16:"010001":MBEDTLS_MD_SHA1:"21026e6800c7fa728fcaaba0d196ae28d7a2ac4ffd8abce794f0985f60c8a6737277365d3fea11db8923a2029a":"f0287413234cc5034724a094c4586b87aff133fc":"07b60e14ec954bfd29e60d0047e789f51d57186c63589903306793ced3f68241c743529aba6a6374f92e19e0163efa33697e196f7661dfaaa47aac6bde5e51deb507c72c589a2ca1693d96b1460381249b2cdb9eac44769f2489c5d3d2f99f0ee3c7ee5bf64a5ac79c42bd433f149be8cb59548361640595513c97af7bc2509723":0

RSAES-OAEP

Decryption Example 5_6

pkcs1_rsaes_oaep_decrypt:1028:16:"03b0d3962f6d17549cbfca11294348dcf0e7e39f8c2bc6824f2164b606d687860dae1e632393cfedf513228229069e2f60e4acd7e633a436063f82385f48993707":16:"02e4c32e2f517269b7072309f00c0e31365f7ce28b236b82912df239abf39572cf0ed604b02982e53564c52d6a05397de5c052a2fddc141ef7189836346aeb331f":16:"0aadf3f9c125e5d891f31ac448e993defe580f802b45f9d7f22ba5021e9c47576b5a1e68031ba9db4e6dabe4d96a1d6f3d267268cff408005f118efcadb99888d1c234467166b2a2b849a05a889c060ac0da0c5fae8b55f309ba62e703742fa0326f2d10b011021489ff497770190d895fd39f52293c39efd73a698bdab9f10ed9":16:"010001":MBEDTLS_MD_SHA1:"541e37b68b6c8872b84c02":"d9fba45c96f21e6e26d29eb2cdcb6585be9cb341":"08c36d4dda33423b2ed6830d85f6411ba1dcf470a1fae0ebefee7c089f256cef74cb96ea69c38f60f39abee44129bcb4c92de7f797623b20074e3d9c2899701ed9071e1efa0bdd84d4c3e5130302d8f0240baba4b84a71cc032f2235a5ff0fae277c3e8f9112bef44c9ae20d175fc9a4058bfc930ba31b02e2e4f444483710f24a":0

RSAES-OAEP

Decryption Example 6_1

pkcs1_rsaes_oaep_decrypt:1029:16:"04a6ce8b7358dfa69bdcf742617005afb5385f5f3a58a24ef74a22a8c05cb7cc38ebd4cc9d9a9d789a62cd0f60f0cb941d3423c9692efa4fe3adff290c4749a38b":16:"0404c9a803371fedb4c5be39f3c00b009e5e08a63be1e40035cdaca5011cc701cf7eebcb99f0ffe17cfd0a4bf7befd2dd536ac946db797fdbc4abe8f29349b91ed":16:"12b17f6dad2ecd19ff46dc13f7860f09e0e0cfb677b38a52592305ceaf022c166db90d04ac29e33f7dd12d9faf66e0816bb63ead267cc7d46c17c37be214bca2a22d723a64e44407436b6fc965729aefc2554f376cd5dcea68293780a62bf39d0029485a160bbb9e5dc0972d21a504f52e5ee028aa416332f510b2e9cff5f722af":16:"010001":MBEDTLS_MD_SHA1:"4046ca8baa3347ca27f49e0d81f9cc1d71be9ba517d4":"dd0f6cfe415e88e5a469a51fbba6dfd40adb4384":"0630eebcd2856c24f798806e41f9e67345eda9ceda386acc9facaea1eeed06ace583709718d9d169fadf414d5c76f92996833ef305b75b1e4b95f662a20faedc3bae0c4827a8bf8a88edbd57ec203a27a841f02e43a615bab1a8cac0701de34debdef62a088089b55ec36ea7522fd3ec8d06b6a073e6df833153bc0aefd93bd1a3":0

RSAES-OAEP

Decryption Example 6_2

pkcs1_rsaes_oaep_decrypt:1029:16:"04a6ce8b7358dfa69bdcf742617005afb5385f5f3a58a24ef74a22a8c05cb7cc38ebd4cc9d9a9d789a62cd0f60f0cb941d3423c9692efa4fe3adff290c4749a38b":16:"0404c9a803371fedb4c5be39f3c00b009e5e08a63be1e40035cdaca5011cc701cf7eebcb99f0ffe17cfd0a4bf7befd2dd536ac946db797fdbc4abe8f29349b91ed":16:"12b17f6dad2ecd19ff46dc13f7860f09e0e0cfb677b38a52592305ceaf022c166db90d04ac29e33f7dd12d9faf66e0816bb63ead267cc7d46c17c37be214bca2a22d723a64e44407436b6fc965729aefc2554f376cd5dcea68293780a62bf39d0029485a160bbb9e5dc0972d21a504f52e5ee028aa416332f510b2e9cff5f722af":16:"010001":MBEDTLS_MD_SHA1:"5cc72c60231df03b3d40f9b57931bc31109f972527f28b19e7480c7288cb3c92b22512214e4be6c914792ddabdf57faa8aa7":"8d14bd946a1351148f5cae2ed9a0c653e85ebd85":"0ebc37376173a4fd2f89cc55c2ca62b26b11d51c3c7ce49e8845f74e7607317c436bc8d23b9667dfeb9d087234b47bc6837175ae5c0559f6b81d7d22416d3e50f4ac533d8f0812f2db9e791fe9c775ac8b6ad0f535ad9ceb23a4a02014c58ab3f8d3161499a260f39348e714ae2a1d3443208fd8b722ccfdfb393e98011f99e63f":0

RSAES-OAEP

Decryption Example 6_3

pkcs1_rsaes_oaep_decrypt:1029:16:"04a6ce8b7358dfa69bdcf742617005afb5385f5f3a58a24ef74a22a8c05cb7cc38ebd4cc9d9a9d789a62cd0f60f0cb941d3423c9692efa4fe3adff290c4749a38b":16:"0404c9a803371fedb4c5be39f3c00b009e5e08a63be1e40035cdaca5011cc701cf7eebcb99f0ffe17cfd0a4bf7befd2dd536ac946db797fdbc4abe8f29349b91ed":16:"12b17f6dad2ecd19ff46dc13f7860f09e0e0cfb677b38a52592305ceaf022c166db90d04ac29e33f7dd12d9faf66e0816bb63ead267cc7d46c17c37be214bca2a22d723a64e44407436b6fc965729aefc2554f376cd5dcea68293780a62bf39d0029485a160bbb9e5dc0972d21a504f52e5ee028aa416332f510b2e9cff5f722af":16:"010001":MBEDTLS_MD_SHA1:"b20e651303092f4bccb43070c0f86d23049362ed96642fc5632c27db4a52e3d831f2ab068b23b149879c002f6bf

3feee97591112562c":"6c075bc45520f165c0bf5ea4c5df191bc9ef0e44":"0a98bf1093619394436cf68d8f38e2f158fde8ea54f3435f239b8d06b8321844202476aeed96009492480ce3a8d705498c4c8c68f01501dc81db608f60087350c8c3b0bd2e9ef6a81458b7c801b89f2e4fe99d4900ba6a4b5e5a96d865dc676c7755928794130d6280a8160a190f2df3ea7cf9aa0271d88e9e6905ecf1c5152d65":0

RSAES-OAEP

Decryption Example 6_4

pkcs1_rsaes_oaep_decrypt:1029:16:"04a6ce8b7358dfa69bdcf742617005afb5385f5f3a58a24ef74a22a8c05cb7cc38ebd4cc9d9a9d789a62cd0f60f0cb941d3423c9692efa4fe3adff290c4749a38b":16:"0404c9a803371fedb4c5be39f3c00b009e5e08a63be1e40035cdaca5011cc701cf7eebcb99f0ffe17cfd0a4bf7befd2dd536ac946db797fdbc4abe8f29349b91ed":16:"12b17f6dad2ecd19ff46dc13f7860f09e0e0cfb677b38a52592305ceaf022c166db90d04ac29e33f7dd12d9faf66e0816bb63ead267cc7d46c17c37be214bca2a22d723a64e44407436b6fc965729aefc2554f376cd5dcea68293780a62bf39d0029485a160bbb9e5dc0972d21a504f52e5ee028aa416332f510b2e9cff5f722af":16:"010001":MBEDTLS_MD_SHA1:"684e3038c5c041f7":"3bbc3bd6637dfe12846901029bf5b0c07103439c":"008e7a67cacfb5c4e24bec7dee149117f19598ce8c45808fef88c608ff9cd6e695263b9a3c0ad4b8ba4c95238e96a8422b8535629c8d5382374479ad13fa39974b242f9a759eeaf9c83ad5a8ca18940a0162ba755876df263f4bd50c6525c56090267c1f0e09ce0899a0cf359e88120abd9bf893445b3cae77d3607359ae9a52f8":0

RSAES-OAEP

Decryption Example 6_5

pkcs1_rsaes_oaep_decrypt:1029:16:"04a6ce8b7358dfa69bdcf742617005afb5385f5f3a58a24ef74a22a8c05cb7cc38ebd4cc9d9a9d789a62cd0f60f0cb941d3423c9692efa4fe3adff290c4749a38b":16:"0404c9a803371fedb4c5be39f3c00b009e5e08a63be1e40035cdaca5011cc701cf7eebcb99f0ffe17cfd0a4bf7befd2dd536ac946db797fdbc4abe8f29349b91ed":16:"12b17f6dad2ecd19ff46dc13f7860f09e0e0cfb677b38a52592305ceaf022c166db90d04ac29e33f7dd12d9faf66e0816bb63ead267cc7d46c17c37be214bca2a22d723a64e44407436b6fc965729aefc2554f376cd5dcea68293780a62bf39d0029485a160bbb9e5dc0972d21a504f52e5ee028aa416332f510b2e9cff5f722af":16:"010001":MBEDTLS_MD_SHA1:"32488cb262d041d6e4dd35f987bf3ca696db1f06ac29a44693":"b46b41893e8bef326f6759383a83071dae7fcabc":"00003474416c7b68bdf961c385737944d7f1f40cb395343c693cc0b4fe63b31fedf1eaeeac9ccc0678b31dc32e0977489514c4f09085f6298a9653f01aea4045ff582ee887be26ae575b73eef7f3774921e375a3d19adda0ca31aa1849887c1f42cac9677f7a2f4e923f6e5a868b38c084ef187594dc9f7f048fea2e02955384ab":0

RSAES-OAEP

Decryption Example 6_6

pkcs1_rsaes_oaep_decrypt:1029:16:"04a6ce8b7358dfa69bdcf742617005afb5385f5f3a58a24ef74a22a8c05cb7cc38ebd4cc9d9a9d789a62cd0f60f0cb941d3423c9692efa4fe3adff290c4749a38b":16:"0404c9a803371fedb4c5be39f3c00b009e5e08a63be1e40035cdaca5011cc701cf7eebcb99f0ffe17cfd0a4bf7befd2dd536ac946db797fdbc4abe8f29349b91ed":16:"12b17f6dad2ecd19ff46dc13f7860f09e0e0cfb677b38a52592305ceaf022c166db90d04ac29e33f7dd12d9faf66e0816bb63ead267cc7d46c17c37be214bca2a22d723a64e44407436b6fc965729aefc2554f376cd5dcea68293780a62bf39d0029485a160bbb9e5dc0972d21a504f52e5ee028aa416332f510b2e9cff5f722af":16:"010001":MBEDTLS_MD_SHA1:"50ba14be8462720279c306ba":"0a2403312a41e3d52f060fbc13a67de5cf7609a7":"0a026dda5fc8785f7bd9bf75327b63e85e2c0fdee5dadb65ebdcac9ae1de95c92c672ab433aa7a8e69ce6a6d8897fac4ac4a54de841ae5e5bbce7687879d79634cea7a30684065c714d52409b928256bbf53eabcd5231eb7259504537399bd29164b726d33a46da701360a4168a091ccab72d44a62fed246c0ffea5b1348ab5470":0

RSAES-OAEP

Decryption Example 7_1

pkcs1_rsaes_oaep_decrypt:1030:16:"0749262c111cd470ec2566e6b3732fc09329469aa19071d3b9c01906514c6f1d26baa14beab0971c8b7e611a4f79009d6fea776928ca25285b0de3643d1a3f8c71":16:"06bc1e50e96c02bf636e9eea8b8

99bbebf7651de77dd474c3e9bc23bad8182b61904c7d97dfbebfb1e00108878b6e67e415391d67942c2b2bf9b4435f88b0cb023":16:"311179f0bcfc9b9d3ca315d00ef30d7bdd3a2cfae9911bfedcb948b3a4782d0732b6ab44aa4bf03741a644dc01bec3e69b01a033e675d8acd7c4925c6b1aec3119051dfd89762d215d45475ffcb59f908148623f37177156f6ae86dd7a7c5f43dc1e1f908254058a284a5f06c0021793a87f1ac5feff7dcaee69c5e51a3789e373":16:"010001":MBEDTLS_MD_SHA1:"47aae909":"43dd09a07ff4cac71caa4632ee5e1c1daee4cd8f":"1688e4ce7794bba6cb7014169ecd559cede2a30b56a52b68d9fe18cf1973ef97b2a03153951c755f6294aa49adbdb55845ab6875fb3986c93ecf927962840d282f9e54ce8b690f7c0cb8bbd73440d9571d1b16cd9260f9eab4783cc482e5223dc60973871783ec27b0ae0fd47732cbc286a173fc92b00fb4ba6824647cd93c85c1":0

RSAES-OAEP

Decryption Example 7_2

pkcs1_rsaes_oaep_decrypt:1030:16:"0749262c111cd470ec2566e6b3732fc09329469aa19071d3b9c01906514c6f1d26baa14beab0971c8b7e611a4f79009d6fea776928ca25285b0de3643d1a3f8c71":16:"06bc1e50e96c02bf636e9eea8b899bbebf7651de77dd474c3e9bc23bad8182b61904c7d97dfbebfb1e00108878b6e67e415391d67942c2b2bf9b4435f88b0cb023":16:"311179f0bcfc9b9d3ca315d00ef30d7bdd3a2cfae9911bfedcb948b3a4782d0732b6ab44aa4bf03741a644dc01bec3e69b01a033e675d8acd7c4925c6b1aec3119051dfd89762d215d45475ffcb59f908148623f37177156f6ae86dd7a7c5f43dc1e1f908254058a284a5f06c0021793a87f1ac5feff7dcaee69c5e51a3789e373":16:"010001":MBEDTLS_MD_SHA1:"1d9b2e2223d9bc13bfb9f162ce735db48ba7c68f6822a0a1a7b6ae165834e7":"3a9c3cec7b84f9bd3adecbc673ec99d54b22bc9b":"1052ed397b2e01e1d0ee1c50bf24363f95e504f4a03434a08fd822574ed6b9736edbb5f390db10321479a8a139350e2bd4977c3778ef331f3e78ae118b268451f20a2f01d471f5d53c566937171b2dbc2d4bde459a5799f0372d6574239b2323d245d0bb81c286b63c89a361017337e4902f88a467f4c7f244bfd5ab46437ff3b6":0

RSAES-OAEP

Decryption Example 7_3

pkcs1_rsaes_oaep_decrypt:1030:16:"0749262c111cd470ec2566e6b3732fc09329469aa19071d3b9c01906514c6f1d26baa14beab0971c8b7e611a4f79009d6fea776928ca25285b0de3643d1a3f8c71":16:"06bc1e50e96c02bf636e9eea8b899bbebf7651de77dd474c3e9bc23bad8182b61904c7d97dfbebfb1e00108878b6e67e415391d67942c2b2bf9b4435f88b0cb023":16:"311179f0bcfc9b9d3ca315d00ef30d7bdd3a2cfae9911bfedcb948b3a4782d0732b6ab44aa4bf03741a644dc01bec3e69b01a033e675d8acd7c4925c6b1aec3119051dfd89762d215d45475ffcb59f908148623f37177156f6ae86dd7a7c5f43dc1e1f908254058a284a5f06c0021793a87f1ac5feff7dcaee69c5e51a3789e373":16:"010001":MBEDTLS_MD_SHA1:"d976fc":"76a75e5b6157a556cf8884bb2e45c293dd545cf5":"2155cd843ff24a4ee8badb7694260028a490813ba8b369a4cbf106ec148e5298707f5965be7d101c1049ea8584c24cd63455ad9c104d686282d3fb803a4c11c1c2e9b91c7178801d1b6640f003f5728df007b8a4ccc92bce05e41a27278d7c85018c52414313a5077789001d4f01910b72aad05d220aa14a58733a7489bc54556b":0

RSAES-OAEP

Decryption Example 7_4

pkcs1_rsaes_oaep_decrypt:1030:16:"0749262c111cd470ec2566e6b3732fc09329469aa19071d3b9c01906514c6f1d26baa14beab0971c8b7e611a4f79009d6fea776928ca25285b0de3643d1a3f8c71":16:"06bc1e50e96c02bf636e9eea8b899bbebf7651de77dd474c3e9bc23bad8182b61904c7d97dfbebfb1e00108878b6e67e415391d67942c2b2bf9b4435f88b0cb023":16:"311179f0bcfc9b9d3ca315d00ef30d7bdd3a2cfae9911bfedcb948b3a4782d0732b6ab44aa4bf03741a644dc01bec3e69b01a033e675d8acd7c4925c6b1aec3119051dfd89762d215d45475ffcb59f908148623f37177156f6ae86dd7a7c5f43dc1e1f908254058a284a5f06c0021793a87f1ac5feff7dcaee69c5e51a3789e373":16:"010001":MBEDTLS_MD_SHA1:"d4738623df223aa43843df8467534c41d013e0c803c624e263666b239bde40a5f29aeb8de79e3daa61dd0370f49bd4b013834b98212aef6b1c5ee373b3cb":"7866314a6ad6f2b250a35941db28f5864b585859":"0ab14c373aeb7d4328d0aaad8c094d88b9eb098b95f21054a29082522be7c27a312878b637917e3d819e6c3c568db5d843802b06d51d9e98a2be0bf40c031423b00edfbff8320efb9171bd2044653a4cb9c5122f6c65e83cda2ec3c126027a9c1a56ba874d0fea23f380b82cf240b8cf540004758c4c77d934157a74f3fc12bfac":0

RSAES-OAEP

Decryption Example 7_5

pkcs1_rsaes_oaep_decrypt:1030:16:"0749262c111cd470ec2566e6b3732fc09329469aa19071d3b9c01906514c6f1d26baa14beab0971c8b7e611a4f79009d6fea776928ca25285b0de3643d1a3f8c71":16:"06bc1e50e96c02bf636e9eea8b899bbebf7651de77dd474c3e9bc23bad8182b61904c7d97dfbebfb1e00108878b6e67e415391d67942c2b2bf9b4435f88b0cb023":16:"311179f0bcfc9b9d3ca315d00ef30d7bdd3a2cfae9911bfedcb948b3a4782d0732b6ab44aa4bf03741a644dc01bec3e69b01a033e675d8acd7c4925c6b1aec3119051dfd89762d215d45475ffcb59f908148623f37177156f6ae86dd7a7c5f43dc1e1f908254058a284a5f06c0021793a87f1ac5feff7dcaee69c5e51a3789e373":16:"010001":MBEDTLS_MD_SHA1:"bb47231ca5ea1d3ad46c99345d9a8a61":"b2166ed472d58db10cab2c6b000cccf10a7dc509":"028387a318277434798b4d97f460068df5298faba5041ba11761a1cb7316b24184114ec500257e2589ed3b607a1ebbe97a6cc2e02bf1b681f42312a33b7a77d8e7855c4a6de03e3c04643f786b91a264a0d6805e2cea91e68177eb7a64d9255e4f27e713b7ccec00dc200ebd21c2ea2bb890feae4942df941dc3f97890ed347478":0

RSAES-OAEP

Decryption Example 7_6

pkcs1_rsaes_oaep_decrypt:1030:16:"0749262c111cd470ec2566e6b3732fc09329469aa19071d3b9c01906514c6f1d26baa14beab0971c8b7e611a4f79009d6fea776928ca25285b0de3643d1a3f8c71":16:"06bc1e50e96c02bf636e9eea8b899bbebf7651de77dd474c3e9bc23bad8182b61904c7d97dfbebfb1e00108878b6e67e415391d67942c2b2bf9b4435f88b0cb023":16:"311179f0bcfc9b9d3ca315d00ef30d7bdd3a2cfae9911bfedcb948b3a4782d0732b6ab44aa4bf03741a644dc01bec3e69b01a033e675d8acd7c4925c6b1aec3119051dfd89762d215d45475ffcb59f908148623f37177156f6ae86dd7a7c5f43dc1e1f908254058a284a5f06c0021793a87f1ac5feff7dcaee69c5e51a3789e373":16:"010001":MBEDTLS_MD_SHA1:"2184827095d35c3f86f600e8e59754013296":"52673bde2ca166c2aa46131ac1dc808d67d7d3b1":"14c678a94ad60525ef39e959b2f3ba5c097a94ff912b67dbace80535c187abd47d075420b1872152bba08f7fc31f313bbf9273c912fc4c0149a9b0cfb79807e346eb332069611bec0ff9bcd168f1f7c33e77313cea454b94e2549eecf002e2acf7f6f2d2845d4fe0aab2e5a92ddf68c480ae11247935d1f62574842216ae674115":0

RSAES-OAEP

Decryption Example 8_1

pkcs1_rsaes_oaep_decrypt:1031:16:"0a02ef8448d9fad8bbd0d004c8c2aa9751ef9721c1b0d03236a54b0df947cbaed5a255ee9e8e20d491ea1723fe094704a9762e88afd16ebb5994412ca966dc4f9f":16:"092d362e7ed3a0bfd9e9fd0e6c0301b6df29159cf50cc83b9b0cf4d6eea71a61e002b46e0ae9f2de62d25b5d7452d498b81c9ac6fc58593d4c3fb4f5d72dfbb0a9":16:"5bdf0e30d321dda5147f882408fa69195480df8f80d3f6e8bf5818504f36427ca9b1f5540b9c65a8f6974cf8447a244d9280201bb49fcbbe6378d1944cd227e230f96e3d10f819dcef276c64a00b2a4b6701e7d01de5fabde3b1e9a0df82f4631359cd22669647fbb1717246134ed7b497cfffbdc42b59c73a96ed90166212dff7":16:"010001":MBEDTLS_MD_SHA1:"050b755e5e6880f7b9e9d692a74c37aae449b31bfea6deff83747a897f6c2c825bb1adbf850a3c96994b5de5b33cbc7d4a17913a7967":"7706ffca1ecfb1ebee2a55e5c6e24cd2797a4125":"09b3683d8a2eb0fb295b62ed1fb9290b714457b7825319f4647872af889b30409472020ad12912bf19b11d4819f49614824ffd84d09c0a17e7d17309d12919790410aa2995699f6a86dbe3242b5acc23af45691080d6b1ae810fb3e3057087f0970092ce00be9562ff4053b6262ce0caa93e13723d2e3a5ba075d45f0d61b54b61":0

RSAES-OAEP

Decryption Example 8_2

pkcs1_rsaes_oaep_decrypt:1031:16:"0a02ef8448d9fad8bbd0d004c8c2aa9751ef9721c1b0d03236a54b0df947cbaed5a255ee9e8e20d491ea1723fe094704a9762e88afd16ebb5994412ca966dc4f9f":16:"092d362e7ed3a0bfd9e9fd0e6c0301b6df29159cf50cc83b9b0cf4d6eea71a61e002b46e0ae9f2de62d25b5d7452d498b81c9ac6fc58593d4c3fb4f5d72dfbb0a9":16:"5bdf0e30d321dda5147f882408fa69195480df8f80d3f6e8bf5818504f36427ca9b1f5540b9c65a8f6974cf8447a244d9280201bb49fcbbe6378d1944cd227e230f96e3d10f819dcef276c64a00b2a4b6701e7d01de5fabde3b1e9a0df8

2f4631359cd22669647fbb1717246134ed7b497cfffbdc42b59c73a96ed90166212dff7":16:"010001":MBEDTLS_MD
_SHA1:"4eb68dcd93ca9b19df111bd43608f557026fe4aa1d5cfac227a3eb5ab9548c18a06dded23f81825986b2fcd711
09ecef7eff88873f075c2aa0c469f69c92bc":"a3717da143b4dcffbc742665a8fa950585548343":"2ecf15c97c5a15b147
6ae986b371b57a24284f4a162a8d0c8182e7905e792256f1812ba5f83f1f7a130e42dcc02232844edc14a31a68ee97ae5
64a383a3411656424c5f62ddb646093c367be1fcda426cf00a06d8acb7e57776fbbd855ac3df506fc16b1d7c3f2110f3d8
068e91e186363831c8409680d8da9ecd8cf1fa20ee39d":0

RSAES-OAEP
Decryption Example 8_3
pkcs1_rsaes_oaep_decrypt:1031:16:"0a02ef8448d9fad8bbd0d004c8c2aa9751ef9721c1b0d03236a54b0df947cbaed5
a255ee9e8e20d491ea1723fe094704a9762e88afd16ebb5994412ca966dc4f9f":16:"092d362e7ed3a0bfd9e9fd0e6c030
1b6df29159cf50cc83b9b0cf4d6eea71a61e002b46e0ae9f2de62d25b5d7452d498b81c9ac6fc58593d4c3fb4f5d72dfbb
0a9":16:"5bdf0e30d321dda5147f882408fa69195480df8f80d3f6e8bf5818504f36427ca9b1f5540b9c65a8f6974cf844
7a244d9280201bb49fcbbe6378d1944cd227e230f96e3d10f819dcef276c64a00b2a4b6701e7d01de5fabde3b1e9a0df8
2f4631359cd22669647fbb1717246134ed7b497cfffbdc42b59c73a96ed90166212dff7":16:"010001":MBEDTLS_MD
_SHA1:"8604ac56328c1ab5ad917861":"ee06209073cca026bb264e5185bf8c68b7739f86":"4bc89130a5b2dabb7c2f
cf90eb5d0eaf9e681b7146a38f3173a3d9cfec52ea9e0a41932e648a9d69344c50da763f51a03c95762131e8052254dcd
2248cba40fd31667786ce05a2b7b531ac9dac9ed584a59b677c1a8aed8c5d15d68c05569e2be780bf7db638fd2bfd2a85
ab276860f3777338fca989ffd743d13ee08e0ca9893f":0

RSAES-OAEP
Decryption Example 8_4
pkcs1_rsaes_oaep_decrypt:1031:16:"0a02ef8448d9fad8bbd0d004c8c2aa9751ef9721c1b0d03236a54b0df947cbaed5
a255ee9e8e20d491ea1723fe094704a9762e88afd16ebb5994412ca966dc4f9f":16:"092d362e7ed3a0bfd9e9fd0e6c030
1b6df29159cf50cc83b9b0cf4d6eea71a61e002b46e0ae9f2de62d25b5d7452d498b81c9ac6fc58593d4c3fb4f5d72dfbb
0a9":16:"5bdf0e30d321dda5147f882408fa69195480df8f80d3f6e8bf5818504f36427ca9b1f5540b9c65a8f6974cf844
7a244d9280201bb49fcbbe6378d1944cd227e230f96e3d10f819dcef276c64a00b2a4b6701e7d01de5fabde3b1e9a0df8
2f4631359cd22669647fbb1717246134ed7b497cfffbdc42b59c73a96ed90166212dff7":16:"010001":MBEDTLS_MD
_SHA1:"fdda5fbf6ec361a9d9a4ac68af216a0686f438b1e0e5c36b955f74e107f39c0dddcc":"990ad573dc48a973235b
6d82543618f2e955105d":"2e456847d8fc36ff0147d6993594b9397227d577752c79d0f904fcb039d4d812fea605a7b5
74dd82ca786f93752348438ee9f5b5454985d5f0e1699e3e7ad175a32e15f03deb042ab9fe1dd9db1bb86f8c089ccb45e
7ef0c5ee7ca9b7290ca6b15bed47039788a8a93ff83e0e8d6244c71006362deef69b6f416fb3c684383fbd0":0

RSAES-OAEP
Decryption Example 8_5
pkcs1_rsaes_oaep_decrypt:1031:16:"0a02ef8448d9fad8bbd0d004c8c2aa9751ef9721c1b0d03236a54b0df947cbaed5
a255ee9e8e20d491ea1723fe094704a9762e88afd16ebb5994412ca966dc4f9f":16:"092d362e7ed3a0bfd9e9fd0e6c030
1b6df29159cf50cc83b9b0cf4d6eea71a61e002b46e0ae9f2de62d25b5d7452d498b81c9ac6fc58593d4c3fb4f5d72dfbb
0a9":16:"5bdf0e30d321dda5147f882408fa69195480df8f80d3f6e8bf5818504f36427ca9b1f5540b9c65a8f6974cf844
7a244d9280201bb49fcbbe6378d1944cd227e230f96e3d10f819dcef276c64a00b2a4b6701e7d01de5fabde3b1e9a0df8
2f4631359cd22669647fbb1717246134ed7b497cfffbdc42b59c73a96ed90166212dff7":16:"010001":MBEDTLS_MD
_SHA1:"4a5f4914bee25de3c69341de07":"ecc63b28f0756f22f52ac8e6ec1251a6ec304718":"1fb9356fd5c4b1796db
2ebf7d0d393cc810adf6145defc2fce714f79d93800d5e2ac211ea8bbecca4b654b94c3b18b30dd576ce34dc95436ef57a
09415645923359a5d7b4171ef22c24670f1b229d3603e91f76671b7df97e7317c97734476d5f3d17d21cf82b5ba9f83df
2e588d36984fd1b584468bd23b2e875f32f68953f7b2":0

RSAES-OAEP

Decryption Example 8_6

pkcs1_rsaes_oaep_decrypt:1031:16:"0a02ef8448d9fad8bbd0d004c8c2aa9751ef9721c1b0d03236a54b0df947cbaed5a255ee9e8e20d491ea1723fe094704a9762e88afd16ebb5994412ca966dc4f9f":16:"092d362e7ed3a0bfd9e9fd0e6c0301b6df29159cf50cc83b9b0cf4d6eea71a61e002b46e0ae9f2de62d25b5d7452d498b81c9ac6fc58593d4c3fb4f5d72dfbb0a9":16:"5bdf0e30d321dda5147f882408fa69195480df8f80d3f6e8bf5818504f36427ca9b1f5540b9c65a8f6974cf8447a244d9280201bb49fcbbe6378d1944cd227e230f96e3d10f819dcef276c64a00b2a4b6701e7d01de5fabde3b1e9a0df82f4631359cd22669647fbb1717246134ed7b497cfffbdc42b59c73a96ed90166212dff7":16:"010001":MBEDTLS_MD_SHA1:"8e07d66f7b880a72563abcd3f35092bc33409fb7f88f2472be":"3925c71b362d40a0a6de42145579ba1e7dd459fc":"3afd9c6600147b21798d818c655a0f4c9212db26d0b0dfdc2a7594ccb3d22f5bf1d7c3e112cd73fc7d509c7a8bafdd3c274d1399009f9609ec4be6477e453f075aa33db382870c1c3409aef392d7386ae3a696b99a94b4da0589447e955d16c98b17602a59bd736279fcd8fb280c4462d590bfa9bf13fed570eafde97330a2c210":0

RSAES-OAEP

Decryption Example 9_1

pkcs1_rsaes_oaep_decrypt:1536:16:"fc8d6c04bec4eb9a8192ca7900cbe536e2e8b519decf33b2459798c6909df4f176db7d23190fc72b8865a718af895f1bcd9145298027423b605e70a47cf58390a8c3e88fc8c48e8b32e3da210dfbe3e881ea5674b6a348c21e93f9e55ea65efd":16:"d200d45e788aacea606a401d0460f87dd5c1027e12dc1a0d7586e8939d9cf789b40f51ac0442961de7d21cc21e05c83155c1f2aa9193387cfdf956cb48d153ba270406f9bbba537d4987d9e2f9942d7a14cbfffea74fecdda928d23e259f5ee1":16:"cf2cd41e34ca3a728ea5cb8aff64c36d27bdef5364e336fd68d3123c5a196a8c287013e853d5156d58d151954520fb4f6d7b17abb6817765909c576119659d902b1906ed8a2b10c155c24d124528dab9eeae379beac66e4a411786dcb8fd0062ebc030de1219a04c2a8c1b7dd3131e4d6b6caee2e31a5ed41ac1509b2ef1ee2ab18364be568ca941c25ecc84ff9d643b5ec1aaae102a20d73f479b780fd6da91075212d9eac03a0674d899eba2e431f4c44b615b6ba2232bd4b33baed73d625d":16:"010001":MBEDTLS_MD_SHA1:"f735fd55ba92592c3b52b8f9c4f69aaa1cbef8fe88add095595412467f9cf4ec0b896c59eda16210e7549c8abb10cdbc21a12ec9b6b5b8fd2f10399eb6":"8ec965f134a3ec9931e92a1ca0dc8169d5ea705c":"267bcd118acab1fc8ba81c85d73003cb8610fa55c1d97da8d48a7c7f06896a4db751aa284255b9d36ad65f37653d829f1b37f97b8001942545b2fc2c55a7376ca7a1be4b1760c8e05a33e5aa2526b8d98e317088e7834c755b2a59b12631a182c05d5d43ab1779264f8456f515ce57dfdf512d5493dab7b7338dc4b7d78db9c091ac3baf537a69fc7f549d979f0eff9a94fda4169bd4d1d19a69c99e33c3b55490d501b39b1edae118ff6793a153261584d3a5f39f6e682e3d17c8cd1261fa72":0

RSAES-OAEP

Decryption Example 9_2

pkcs1_rsaes_oaep_decrypt:1536:16:"fc8d6c04bec4eb9a8192ca7900cbe536e2e8b519decf33b2459798c6909df4f176db7d23190fc72b8865a718af895f1bcd9145298027423b605e70a47cf58390a8c3e88fc8c48e8b32e3da210dfbe3e881ea5674b6a348c21e93f9e55ea65efd":16:"d200d45e788aacea606a401d0460f87dd5c1027e12dc1a0d7586e8939d9cf789b40f51ac0442961de7d21cc21e05c83155c1f2aa9193387cfdf956cb48d153ba270406f9bbba537d4987d9e2f9942d7a14cbfffea74fecdda928d23e259f5ee1":16:"cf2cd41e34ca3a728ea5cb8aff64c36d27bdef5364e336fd68d3123c5a196a8c287013e853d5156d58d151954520fb4f6d7b17abb6817765909c576119659d902b1906ed8a2b10c155c24d124528dab9eeae379beac66e4a411786dcb8fd0062ebc030de1219a04c2a8c1b7dd3131e4d6b6caee2e31a5ed41ac1509b2ef1ee2ab18364be568ca941c25ecc84ff9d643b5ec1aaae102a20d73f479b780fd6da91075212d9eac03a0674d899eba2e431f4c44b615b6ba2232bd4b33baed73d625d":16:"010001":MBEDTLS_MD_SHA1:"81b906605015a63aabe42ddf11e1978912f5404c7474b26dce3ed482bf961ecc818bf420c54659":"ecb1b8b25fa50cdab08e56042867f4af5826d16c":"93ac9f0671ec29acbb444effc1a5741351d60fdb0e393fbf754acf0de49761a14841df7772e9bc82773966a1584c4d72baea00118f83f35cca6e537cbd4d811f5583b29783d8a6d94cd31be70d6f526c10ff09c6fa7ce069795a3fcd0511fd5fcb564bcc80ea9c78f38b80012539d8a4ddf6fe81e9cddb7f50dbbbbcc7e5d86097ccf4ec49189fb8bf318be6d5a0715d516b49af191258cd32dc833ce6eb4673c03a19bbace88cc54895f636cc0c1ec89096d11ce235a265ca1764232a689ae8":0

RSAES-OAEP

Decryption Example 9_3

pkcs1_rsaes_oaep_decrypt:1536:16:"fc8d6c04bec4eb9a8192ca7900cbe536e2e8b519decf33b2459798c6909df4f176db7d23190fc72b8865a718af895f1bcd9145298027423b605e70a47cf58390a8c3e88fc8c48e8b32e3da210dfbe3e881ea5674b6a348c21e93f9e55ea65efd":16:"d200d45e788aacea606a401d0460f87dd5c1027e12dc1a0d7586e8939d9cf789b40f51ac0442961de7d21cc21e05c83155c1f2aa9193387cfdf956cb48d153ba270406f9bbba537d4987d9e2f9942d7a14cbfffea74fecdda928d23e259f5ee1":16:"cf2cd41e34ca3a728ea5cb8aff64c36d27bdef5364e336fd68d3123c5a196a8c287013e853d5156d58d151954520fb4f6d7b17abb6817765909c576119659d902b1906ed8a2b10c155c24d124528dab9eeae379beac66e4a411786dcb8fd0062ebc030de1219a04c2a8c1b7dd3131e4d6b6caee2e31a5ed41ac1509b2ef1ee2ab18364be568ca941c25ecc84ff9d643b5ec1aaae102a20d73f479b780fd6da91075212d9eac03a0674d899eba2e431f4c44b615b6ba2232bd4b33baed73d625d":16:"010001":MBEDTLS_MD_SHA1:"fd326429df9b890e09b54b18b8f34f1e24":"e89bb032c6ce622cbdb53bc9466014ea77f777c0":"81ebdd95054b0c822ef9ad7693f5a87adfb4b4c4ce70df2df84ed49c04da58ba5fc20a19e1a6e8b7a3900b22796dc4e869ee6b42792d15a8eceb56c09c69914e813cea8f6931e4b8ed6f421af298d595c97f4789c7caa612c7ef360984c21b93edc5401068b5af4c78a8771b984d53b8ea8adf2f6a7d4a0ba76c75e1dd9f658f20ded4a46071d46d7791b56803d8fea7f0b0f8e41ae3f09383a6f9585fe7753eaaffd2bf94563108beecc207bbb535f5fcc705f0dde9f708c62f49a9c90371d3":0

RSAES-OAEP

Decryption Example 9_4

pkcs1_rsaes_oaep_decrypt:1536:16:"fc8d6c04bec4eb9a8192ca7900cbe536e2e8b519decf33b2459798c6909df4f176db7d23190fc72b8865a718af895f1bcd9145298027423b605e70a47cf58390a8c3e88fc8c48e8b32e3da210dfbe3e881ea5674b6a348c21e93f9e55ea65efd":16:"d200d45e788aacea606a401d0460f87dd5c1027e12dc1a0d7586e8939d9cf789b40f51ac0442961de7d21cc21e05c83155c1f2aa9193387cfdf956cb48d153ba270406f9bbba537d4987d9e2f9942d7a14cbfffea74fecdda928d23e259f5ee1":16:"cf2cd41e34ca3a728ea5cb8aff64c36d27bdef5364e336fd68d3123c5a196a8c287013e853d5156d58d151954520fb4f6d7b17abb6817765909c576119659d902b1906ed8a2b10c155c24d124528dab9eeae379beac66e4a411786dcb8fd0062ebc030de1219a04c2a8c1b7dd3131e4d6b6caee2e31a5ed41ac1509b2ef1ee2ab18364be568ca941c25ecc84ff9d643b5ec1aaae102a20d73f479b780fd6da91075212d9eac03a0674d899eba2e431f4c44b615b6ba2232bd4b33baed73d625d":16:"010001":MBEDTLS_MD_SHA1:"f1459b5f0c92f01a0f723a2e5662484d8f8c0a20fc29dad6acd43bb5f3effdf4e1b63e07fdfe6628d0d74ca19bf2d69e4a0abf86d293925a796772f8088e":"606f3b99c0b9ccd771eaa29ea0e4c884f3189ccc":"bcc35f94cde66cb1136625d625b94432a35b22f3d2fa11a613ff0fca5bd57f87b902ccdc1cd0aebcb0715ee869d1d1fe395f6793003f5eca465059c88660d446ff5f0818552022557e38c08a67ead991262254f10682975ec56397768537f4977af6d5f6aaceb7fb25dec5937230231fd8978af49119a29f29e424ab8272b47562792d5c94f774b8829d0b0d9f1a8c9eddf37574d5fa248eefa9c5271fc5ec2579c81bdd61b410fa61fe36e424221c113addb275664c801d34ca8c6351e4a858":0

RSAES-OAEP

Decryption Example 9_5

pkcs1_rsaes_oaep_decrypt:1536:16:"fc8d6c04bec4eb9a8192ca7900cbe536e2e8b519decf33b2459798c6909df4f176db7d23190fc72b8865a718af895f1bcd9145298027423b605e70a47cf58390a8c3e88fc8c48e8b32e3da210dfbe3e881ea5674b6a348c21e93f9e55ea65efd":16:"d200d45e788aacea606a401d0460f87dd5c1027e12dc1a0d7586e8939d9cf789b40f51ac0442961de7d21cc21e05c83155c1f2aa9193387cfdf956cb48d153ba270406f9bbba537d4987d9e2f9942d7a14cbfffea74fecdda928d23e259f5ee1":16:"cf2cd41e34ca3a728ea5cb8aff64c36d27bdef5364e336fd68d3123c5a196a8c287013e853d5156d58d151954520fb4f6d7b17abb6817765909c576119659d902b1906ed8a2b10c155c24d124528dab9eeae379beac66e4a411786dcb8fd0062ebc030de1219a04c2a8c1b7dd3131e4d6b6caee2e31a5ed41ac1509b2ef1ee2ab18364be568ca941c25ecc84ff9d643b5ec1aaae102a20d73f479b780fd6da91075212d9eac03a0674d899eba2e431f4c44b615b6ba2232bd4b33baed73d625d":16:"010001":MBEDTLS_MD_SHA1:"53e6e8c729d6f9c319dd317e74b0db8e4ccca25f3c8305746e137ac63a63ef3739e7b595abb96e8d55e54f7bd41ab433378ffb911d":"fcbc421402e9ecabc6082afa40ba5f26522c840e":"232afbc927fa08c2f6a27b87d4a5cb09c07dc26fae73d73a90558839f4fd66d281b87ec734bce237ba166698ed829106a7de6942cd6cdce78fed8d2e4d81428e66490d036264cef92af941d3e35055fe3981e14d29

cbb9a4f67473063baec79a1179f5a17c9c1832f2838fd7d5e59bb9659d56dce8a019edef1bb3accc697cc6cc7a778f60a0
64c7f6f5d529c6210262e003de583e81e3167b89971fb8c0e15d44fffef89b53d8d64dd797d159b56d2b08ea5307ea12c
241bd58d4ee278a1f2e":0

RSAES-OAEP
Decryption Example 9_6
pkcs1_rsaes_oaep_decrypt:1536:16:"fc8d6c04bec4eb9a8192ca7900cbe536e2e8b519decf33b2459798c6909df4f176
db7d23190fc72b8865a718af895f1bcd9145298027423b605e70a47cf58390a8c3e88fc8c48e8b32e3da210dfbe3e881e
a5674b6a348c21e93f9e55ea65efd":16:"d200d45e788aacea606a401d0460f87dd5c1027e12dc1a0d7586e8939d9cf78
9b40f51ac0442961de7d21cc21e05c83155c1f2aa9193387cfdf956cb48d153ba270406f9bbba537d4987d9e2f9942d7a
14cbfffea74fecdda928d23e259f5ee1":16:"cf2cd41e34ca3a728ea5cb8aff64c36d27bdef5364e336fd68d3123c5a196a
8c287013e853d5156d58d151954520fb4f6d7b17abb6817765909c576119659d902b1906ed8a2b10c155c24d124528d
ab9eeae379beac66e4a411786dcb8fd0062ebc030de1219a04c2a8c1b7dd3131e4d6b6caee2e31a5ed41ac1509b2ef1ee
2ab18364be568ca941c25ecc84ff9d643b5ec1aaae102a20d73f479b780fd6da91075212d9eac03a0674d899eba2e431f
4c44b615b6ba2232bd4b33baed73d625d":16:"010001":MBEDTLS_MD_SHA1:"b6b28ea2198d0c1008bc64":"23aa
de0e1e08bb9b9a78d2302a52f9c21b2e1ba2":"438cc7dc08a68da249e42505f8573ba60e2c2773d5b290f4cf9dff718e8
42081c383e67024a0f29594ea987b9d25e4b738f285970d195abb3a8c8054e3d79d6b9c9a8327ba596f1259e27126674
766907d8d582ff3a8476154929adb1e6d1235b2ccb4ec8f663ba9cc670a92bebd853c8dbf69c6436d016f61add836e947
32450434207f9fd4c43dec2a12a958efa01efe2669899b5e604c255c55fb7166de5589e369597bb09168c06dd5db177e0
6a1740eb2d5c82faeca6d92fcee9931ba9f":0

RSAES-OAEP
Decryption Example 10_1
pkcs1_rsaes_oaep_decrypt:2048:16:"ecf5aecd1e5515fffacbd75a2816c6ebf49018cdfb4638e185d66a7396b6f8090f8
018c7fd95cc34b857dc17f0cc6516bb1346ab4d582cadad7b4103352387b70338d084047c9d9539b6496204b3dd6ea4
42499207bec01f964287ff6336c3984658336846f56e46861881c10233d2176bf15a5e96ddc780bc868aa77d3ce769":1
6:"bc46c464fc6ac4ca783b0eb08a3c841b772f7e9b2f28babd588ae885e1a0c61e4858a0fb25ac299990f35be85164c25
9ba1175cdd7192707135184992b6c29b746dd0d2cabe142835f7d148cc161524b4a09946d48b828473f1ce76b6cb688
6c345c03e05f41d51b5c3a90a3f24073c7d74a4fe25d9cf21c75960f3fc3863183":16:"ae45ed5601cec6b8cc05f803935
c674ddbe0d75c4c09fd7951fc6b0caec313a8df39970c518bffba5ed68f3f0d7f22a4029d413f1ae07e4ebe9e4177ce23e7
f5404b569e4ee1bdcf3c1fb03ef113802d4f855eb9b5134b5a7c8085adcae6fa2fa1417ec3763be171b0c62b760ede23c1
2ad92b980884c641f5a8fac26bdad4a03381a22fe1b754885094c82506d4019a535a286afeb271bb9ba592de18dcf600c
2aeeae56e02f7cf79fc14cf3bdc7cd84febbbf950ca90304b2219a7aa063aefa2c3c1980e560cd64afe779585b6107657b9
57857efde6010988ab7de417fc88d8f384c4e6e72c3f943e0c31c0c4a5cc36f879d8a3ac9d7d59860eaada6b83bb":16:"0
10001":MBEDTLS_MD_SHA1:"8bba6bf82a6c0f86d5f1756e97956870b08953b06b4eb205bc1694ee":"47e1ab7119
fee56c95ee5eaad86f40d0aa63bd33":"53ea5dc08cd260fb3b858567287fa91552c30b2febfba213f0ae87702d068d19ba
b07fe574523dfb42139d68c3c5afeee0bfe4cb7969cbf382b804d6e61396144e2d0e60741f8993c3014b58b9b1957a8ba
bcd23af854f4c356fb1662aa72bfcc7e586559dc4280d160c126785a723ebeebeff71f11594440aaef87d10793a8774a23
9d4a04c87fe1467b9daf85208ec6c7255794a96cc29142f9a8bd418e3c1fd67344b0cd0829df3b2bec60253196293c6b3
4d3f75d32f213dd45c6273d505adf4cced1057cb758fc26aeefa441255ed4e64c199ee075e7f16646182fdb464739b68a
b5daff0e63e9552016824f054bf4d3c8c90a97bb6b6553284eb429fcc":0

RSAES-OAEP
Decryption Example 10_2
pkcs1_rsaes_oaep_decrypt:2048:16:"ecf5aecd1e5515fffacbd75a2816c6ebf49018cdfb4638e185d66a7396b6f8090f8
018c7fd95cc34b857dc17f0cc6516bb1346ab4d582cadad7b4103352387b70338d084047c9d9539b6496204b3dd6ea4
42499207bec01f964287ff6336c3984658336846f56e46861881c10233d2176bf15a5e96ddc780bc868aa77d3ce769":1
6:"bc46c464fc6ac4ca783b0eb08a3c841b772f7e9b2f28babd588ae885e1a0c61e4858a0fb25ac299990f35be85164c25

9ba1175cdd7192707135184992b6c29b746dd0d2cabe142835f7d148cc161524b4a09946d48b828473f1ce76b6cb688
6c345c03e05f41d51b5c3a90a3f24073c7d74a4fe25d9cf21c75960f3fc3863183":16:"ae45ed5601cec6b8cc05f803935
c674ddbe0d75c4c09fd7951fc6b0caec313a8df39970c518bffba5ed68f3f0d7f22a4029d413f1ae07e4ebe9e4177ce23e7
f5404b569e4ee1bdcf3c1fb03ef113802d4f855eb9b5134b5a7c8085adcae6fa2fa1417ec3763be171b0c62b760ede23c1
2ad92b980884c641f5a8fac26bdad4a03381a22fe1b754885094c82506d4019a535a286afeb271bb9ba592de18dcf600c
2aeeae56e02f7cf79fc14cf3bdc7cd84febbbf950ca90304b2219a7aa063aefa2c3c1980e560cd64afe779585b6107657b9
57857efde6010988ab7de417fc88d8f384c4e6e72c3f943e0c31c0c4a5cc36f879d8a3ac9d7d59860eaada6b83bb":16:"0
10001":MBEDTLS_MD_SHA1:"e6ad181f053b58a904f2457510373e57":"6d17f5b4c1ffac351d195bf7b09d09f09a4
079cf":"a2b1a430a9d657e2fa1c2bb5ed43ffb25c05a308fe9093c01031795f5874400110828ae58fb9b581ce9dddd3e5
49ae04a0985459bde6c626594e7b05dc4278b2a1465c1368408823c85e96dc66c3a30983c639664fc4569a37fe21e5a1
95b5776eed2df8d8d361af686e750229bbd663f161868a50615e0c337bec0ca35fec0bb19c36eb2e0bbcc0582fa1d93aa
cdb061063f59f2ce1ee43605e5d89eca183d2acdfe9f81011022ad3b43a3dd417dac94b4e11ea81b192966e966b182082
e71964607b4f8002f36299844a11f2ae0faeac2eae70f8f4f98088acdcd0ac556e9fccc511521908fad26f04c6420145030
5778758b0538bf8b5bb144a828e629795":0

RSAES-OAEP

Decryption Example 10_3

pkcs1_rsaes_oaep_decrypt:2048:16:"ecf5aecd1e5515fffacbd75a2816c6ebf49018cdfb4638e185d66a7396b6f8090f8
018c7fd95cc34b857dc17f0cc6516bb1346ab4d582cadad7b4103352387b70338d084047c9d9539b6496204b3dd6ea4
42499207bec01f964287ff6336c3984658336846f56e46861881c10233d2176bf15a5e96ddc780bc868aa77d3ce769":1
6:"bc46c464fc6ac4ca783b0eb08a3c841b772f7e9b2f28babd588ae885e1a0c61e4858a0fb25ac299990f35be85164c25
9ba1175cdd7192707135184992b6c29b746dd0d2cabe142835f7d148cc161524b4a09946d48b828473f1ce76b6cb688
6c345c03e05f41d51b5c3a90a3f24073c7d74a4fe25d9cf21c75960f3fc3863183":16:"ae45ed5601cec6b8cc05f803935
c674ddbe0d75c4c09fd7951fc6b0caec313a8df39970c518bffba5ed68f3f0d7f22a4029d413f1ae07e4ebe9e4177ce23e7
f5404b569e4ee1bdcf3c1fb03ef113802d4f855eb9b5134b5a7c8085adcae6fa2fa1417ec3763be171b0c62b760ede23c1
2ad92b980884c641f5a8fac26bdad4a03381a22fe1b754885094c82506d4019a535a286afeb271bb9ba592de18dcf600c
2aeeae56e02f7cf79fc14cf3bdc7cd84febbbf950ca90304b2219a7aa063aefa2c3c1980e560cd64afe779585b6107657b9
57857efde6010988ab7de417fc88d8f384c4e6e72c3f943e0c31c0c4a5cc36f879d8a3ac9d7d59860eaada6b83bb":16:"0
10001":MBEDTLS_MD_SHA1:"510a2cf60e866fa2340553c94ea39fbc256311e83e94454b4124":"385387514deccc
7c740dd8cdf9daee49a1cbfd54":"9886c3e6764a8b9a84e84148ebd8c3b1aa8050381a78f668714c16d9cfd2a6edc5697
9c535d9dee3b44b85c18be8928992371711472216d95dda98d2ee8347c9b14dffdff84aa48d25ac06f7d7e65398ac967b
1ce90925f67dce049b7f812db0742997a74d44fe81dbe0e7a3feaf2e5c40af888d550ddbbe3bc20657a29543f8fc2913b9
bd1a61b2ab2256ec409bbd7dc0d17717ea25c43f42ed27df8738bf4afc6766ff7aff0859555ee283920f4c8a63c4a7340c
bafddc339ecdb4b0515002f96c932b5b79167af699c0ad3fccfdf0f44e85a70262bf2e18fe34b850589975e867ff969d48e
abf212271546cdc05a69ecb526e52870c836f307bd798780ede":0

RSAES-OAEP

Decryption Example 10_4

pkcs1_rsaes_oaep_decrypt:2048:16:"ecf5aecd1e5515fffacbd75a2816c6ebf49018cdfb4638e185d66a7396b6f8090f8
018c7fd95cc34b857dc17f0cc6516bb1346ab4d582cadad7b4103352387b70338d084047c9d9539b6496204b3dd6ea4
42499207bec01f964287ff6336c3984658336846f56e46861881c10233d2176bf15a5e96ddc780bc868aa77d3ce769":1
6:"bc46c464fc6ac4ca783b0eb08a3c841b772f7e9b2f28babd588ae885e1a0c61e4858a0fb25ac299990f35be85164c25
9ba1175cdd7192707135184992b6c29b746dd0d2cabe142835f7d148cc161524b4a09946d48b828473f1ce76b6cb688
6c345c03e05f41d51b5c3a90a3f24073c7d74a4fe25d9cf21c75960f3fc3863183":16:"ae45ed5601cec6b8cc05f803935
c674ddbe0d75c4c09fd7951fc6b0caec313a8df39970c518bffba5ed68f3f0d7f22a4029d413f1ae07e4ebe9e4177ce23e7
f5404b569e4ee1bdcf3c1fb03ef113802d4f855eb9b5134b5a7c8085adcae6fa2fa1417ec3763be171b0c62b760ede23c1
2ad92b980884c641f5a8fac26bdad4a03381a22fe1b754885094c82506d4019a535a286afeb271bb9ba592de18dcf600c
2aeeae56e02f7cf79fc14cf3bdc7cd84febbbf950ca90304b2219a7aa063aefa2c3c1980e560cd64afe779585b6107657b9

57857efde6010988ab7de417fc88d8f384c4e6e72c3f943e0c31c0c4a5cc36f879d8a3ac9d7d59860eaada6b83bb":16:"0
10001":MBEDTLS_MD_SHA1:"bcdd190da3b7d300df9a06e22caae2a75f10c91ff667b7c16bde8b53064a2649a9404
5c9":"5caca6a0f764161a9684f85d92b6e0ef37ca8b65":"6318e9fb5c0d05e5307e1683436e903293ac4642358aaa223
d7163013aba87e2dfda8e60c6860e29a1e92686163ea0b9175f329ca3b131a1edd3a77759a8b97bad6a4f8f4396f28cf6f
39ca58112e48160d6e203daa5856f3aca5ffed577af499408e3dfd233e3e604dbe34a9c4c9082de65527cac6331d29dc8
0e0508a0fa7122e7f329f6cca5cfa34d4d1da417805457e008bec549e478ff9e12a763c477d15bbb78f5b69bd57830fc2c
4ed686d79bc72a95d85f88134c6b0afe56a8ccfbc855828bb339bd17909cf1d70de3335ae07039093e606d655365de65
50b872cd6de1d440ee031b61945f629ad8a353b0d40939e96a3c450d2a8d5eee9f678093c8":0

RSAES-OAEP

Decryption Example 10_5

pkcs1_rsaes_oaep_decrypt:2048:16:"ecf5aecd1e5515fffacbd75a2816c6ebf49018cdfb4638e185d66a7396b6f8090f8
018c7fd95cc34b857dc17f0cc6516bb1346ab4d582cadad7b4103352387b70338d084047c9d9539b6496204b3dd6ea4
42499207bec01f964287ff6336c3984658336846f56e46861881c10233d2176bf15a5e96ddc780bc868aa77d3ce769":1
6:"bc46c464fc6ac4ca783b0eb08a3c841b772f7e9b2f28babd588ae885e1a0c61e4858a0fb25ac299990f35be85164c25
9ba1175cdd7192707135184992b6c29b746dd0d2cabe142835f7d148cc161524b4a09946d48b828473f1ce76b6cb688
6c345c03e05f41d51b5c3a90a3f24073c7d74a4fe25d9cf21c75960f3fc3863183":16:"ae45ed5601cec6b8cc05f803935
c674ddbe0d75c4c09fd7951fc6b0caec313a8df39970c518bffba5ed68f3f0d7f22a4029d413f1ae07e4ebe9e4177ce23e7
f5404b569e4ee1bdcf3c1fb03ef113802d4f855eb9b5134b5a7c8085adcae6fa2fa1417ec3763be171b0c62b760ede23c1
2ad92b980884c641f5a8fac26bdad4a03381a22fe1b754885094c82506d4019a535a286afeb271bb9ba592de18dcf600c
2aeeae56e02f7cf79fc14cf3bdc7cd84febbbf950ca90304b2219a7aa063aefa2c3c1980e560cd64afe779585b6107657b9
57857efde6010988ab7de417fc88d8f384c4e6e72c3f943e0c31c0c4a5cc36f879d8a3ac9d7d59860eaada6b83bb":16:"0
10001":MBEDTLS_MD_SHA1:"a7dd6c7dc24b46f9dd5f1e91ada4c3b3df947e877232a9":"95bca9e3859894b3dd86
9fa7ecd5bbc6401bf3e4":"75290872ccfd4a4505660d651f56da6daa09ca1301d890632f6a992f3d565cee464afded40e
d3b5be9356714ea5aa7655f4a1366c2f17c728f6f2c5a5d1f8e28429bc4e6f8f2cff8da8dc0e0a9808e45fd09ea2fa40cb2
b6ce6ffff5c0e159d11b68d90a85f7b84e103b09e682666480c657505c0929259468a314786d74eab131573cf234bf57d
b7d9e66cc6748192e002dc0deea930585f0831fdcd9bc33d51f79ed2ffc16bcf4d59812fcebcaa3f9069b0e445686d644c
25ccf63b456ee5fa6ffe96f19cdf751fed9eaf35957754dbf4bfea5216aa1844dc507cb2d080e722eba150308c2b5ff1193
620f1766ecf4481bafb943bd292877f2136ca494aba0":0

RSAES-OAEP

Decryption Example 10_6

pkcs1_rsaes_oaep_decrypt:2048:16:"ecf5aecd1e5515fffacbd75a2816c6ebf49018cdfb4638e185d66a7396b6f8090f8
018c7fd95cc34b857dc17f0cc6516bb1346ab4d582cadad7b4103352387b70338d084047c9d9539b6496204b3dd6ea4
42499207bec01f964287ff6336c3984658336846f56e46861881c10233d2176bf15a5e96ddc780bc868aa77d3ce769":1
6:"bc46c464fc6ac4ca783b0eb08a3c841b772f7e9b2f28babd588ae885e1a0c61e4858a0fb25ac299990f35be85164c25
9ba1175cdd7192707135184992b6c29b746dd0d2cabe142835f7d148cc161524b4a09946d48b828473f1ce76b6cb688
6c345c03e05f41d51b5c3a90a3f24073c7d74a4fe25d9cf21c75960f3fc3863183":16:"ae45ed5601cec6b8cc05f803935
c674ddbe0d75c4c09fd7951fc6b0caec313a8df39970c518bffba5ed68f3f0d7f22a4029d413f1ae07e4ebe9e4177ce23e7
f5404b569e4ee1bdcf3c1fb03ef113802d4f855eb9b5134b5a7c8085adcae6fa2fa1417ec3763be171b0c62b760ede23c1
2ad92b980884c641f5a8fac26bdad4a03381a22fe1b754885094c82506d4019a535a286afeb271bb9ba592de18dcf600c
2aeeae56e02f7cf79fc14cf3bdc7cd84febbbf950ca90304b2219a7aa063aefa2c3c1980e560cd64afe779585b6107657b9
57857efde6010988ab7de417fc88d8f384c4e6e72c3f943e0c31c0c4a5cc36f879d8a3ac9d7d59860eaada6b83bb":16:"0
10001":MBEDTLS_MD_SHA1:"eaf1a73a1b0c4609537de69cd9228bbcfb9a8ca8c6c3efaf056fe4a7f4634ed00b7c39
ec6922d7b8ea2c04ebac":"9f47ddf42e97eea856a9bdbc714eb3ac22f6eb32":"2d207a73432a8fb4c03051b3f73b28a61
764098dfa34c47a20995f8115aa6816679b557e82dbee584908c6e69782d7deb34dbd65af063d57fca76a5fd069492fd6
068d9984d209350565a62e5c77f23038c12cb10c6634709b547c46f6b4a709bd85ca122d74465ef97762c29763e06dbc
7a9e738c78bfca0102dc5e79d65b973f28240caab2e161a78b57d262457ed8195d53e3c7ae9da021883c6db7c24afdd2

322eac972ad3c354c5fcef1e146c3a0290fb67adf007066e00428d2cec18ce58f9328698defef4b2eb5ec76918fde1c198c
bb38b7afc67626a9aefec4322bfd90d2563481c9a221f78c8272c82d1b62ab914e1c69f6af6ef30ca5260db4a46":0

RSASSA-PSS
Signing Test Vector Int
pkcs1_rsassa_pss_sign:1024:16:"d17f655bf27c8b16d35462c905cc04a26f37e2a67fa9c0ce0dced472394a0df743fe7f
929e378efdb368eddff453cf007af6d948e0ade757371f8a711e278f6b":16:"c6d92b6fee7414d1358ce1546fb62987530
b90bd15e0f14963a5e2635adb69347ec0c01b2ab1763fd8ac1a592fb22757463a982425bb97a3a437c5bf86d03f2f":16:
"a2ba40ee07e3b2bd2f02ce227f36a195024486e49c19cb41bbbdfbba98b22b0e577c2eeaffa20d883a76e65e394c69d4
b3c05a1e8fadda27edb2a42bc000fe888b9b32c22d15add0cd76b3e7936e19955b220dd17d4ea904b1ec102b2e4de775
1222aa99151024c7cb41cc5ea21d00eeb41f7c800834d2c6e06bce3bce7ea9a5":16:"010001":MBEDTLS_MD_SHA1
:MBEDTLS_MD_SHA1:"859eef2fd78aca00308bdc471193bf55bf9d78db8f8a672b484634f3c9c26e6478ae10260fe
0dd8c082e53a5293af2173cd50c6d5d354febf78b26021c25c02712e78cd4694c9f469777e451e7f8e9e04cd3739c6bbf
edae487fb55644e9ca74ff77a53cb729802f6ed4a5ffa8ba159890fc":"e3b5d5d002c1bce50c2b65ef88a188d83bce7e61
":"8daa627d3de7595d63056c7ec659e54406f10610128baae821c8b2a0f3936d54dc3bdce46689f6b7951bb18e840542
769718d5715d210d85efbb596192032c42be4c29972c856275eb6d5a45f05f51876fc6743deddd28caec9bb30ea99e02
c3488269604fe497f74ccd7c7fca1671897123cbd30def5d54a2b5536ad90a747e":0

RSASSA-PSS
Verification Test Vector Int
pkcs1_rsassa_pss_verify:1024:16:"a2ba40ee07e3b2bd2f02ce227f36a195024486e49c19cb41bbbdfbba98b22b0e577
c2eeaffa20d883a76e65e394c69d4b3c05a1e8fadda27edb2a42bc000fe888b9b32c22d15add0cd76b3e7936e19955b22
0dd17d4ea904b1ec102b2e4de7751222aa99151024c7cb41cc5ea21d00eeb41f7c800834d2c6e06bce3bce7ea9a5":16:"
010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"859eef2fd78aca00308bdc471193bf55bf9d78db8f8a672
b484634f3c9c26e6478ae10260fe0dd8c082e53a5293af2173cd50c6d5d354febf78b26021c25c02712e78cd4694c9f46
9777e451e7f8e9e04cd3739c6bbfedae487fb55644e9ca74ff77a53cb729802f6ed4a5ffa8ba159890fc":"e3b5d5d002c1
bce50c2b65ef88a188d83bce7e61":"8daa627d3de7595d63056c7ec659e54406f10610128baae821c8b2a0f3936d54dc
3bdce46689f6b7951bb18e840542769718d5715d210d85efbb596192032c42be4c29972c856275eb6d5a45f05f51876f
c6743deddd28caec9bb30ea99e02c3488269604fe497f74ccd7c7fca1671897123cbd30def5d54a2b5536ad90a747e":0

RSASSA-PSS
Signing Test Vector Hash too large
pkcs1_rsassa_pss_sign:1024:16:"d17f655bf27c8b16d35462c905cc04a26f37e2a67fa9c0ce0dced472394a0df743fe7f
929e378efdb368eddff453cf007af6d948e0ade757371f8a711e278f6b":16:"c6d92b6fee7414d1358ce1546fb62987530
b90bd15e0f14963a5e2635adb69347ec0c01b2ab1763fd8ac1a592fb22757463a982425bb97a3a437c5bf86d03f2f":16:
"a2ba40ee07e3b2bd2f02ce227f36a195024486e49c19cb41bbbdfbba98b22b0e577c2eeaffa20d883a76e65e394c69d4
b3c05a1e8fadda27edb2a42bc000fe888b9b32c22d15add0cd76b3e7936e19955b220dd17d4ea904b1ec102b2e4de775
1222aa99151024c7cb41cc5ea21d00eeb41f7c800834d2c6e06bce3bce7ea9a5":16:"010001":MBEDTLS_MD_SHA1
:MBEDTLS_MD_SHA512:"d436e99569fd32a7c8a05bbc90d32c49d436e99569fd32a7c8a05bbc90d32c49d436e995
69fd32a7c8a05bbc90d32c49d436e99569fd32a7c8a05bbc90d32c49d436e99569fd32a7c8a05bbc90d32c49d436e995
69fd00":"e3b5d5d002c1bce50c2b65ef88a188d83bce7e61":"":MBEDTLS_ERR_RSA_BAD_INPUT_DATA

RSASSA-PSS
Signature Example 1_1
pkcs1_rsassa_pss_sign:1024:16:"e7e8942720a877517273a356053ea2a1bc0c94aa72d55c6e86296b2dfc967948c0a7
2cbccca7eacb35706e09a1df55a1535bd9b3cc34160b3b6dcd3eda8e6443":16:"b69dca1cf7d4d7ec81e75b90fcca874a
bcde123fd2700180aa90479b6e48de8d67ed24f9f19d85ba275874f542cd20dc723e6963364a1f9425452b269a6799fd"
:16:"a56e4a0e701017589a5187dc7ea841d156f2ec0e36ad52a44dfeb1e61f7ad991d8c51056ffedb162b4c0f283a12a88

a394dff526ab7291cbb307ceabfce0b1dfd5cd9508096d5b2b8b6df5d671ef6377c0921cb23c270a70e2598e6ff89d19f1
05acc2d3f0cb35f29280e1386b6f64c4ef22e1e1f20d0ce8cffb2249bd9a2137":16:"010001":MBEDTLS_MD_SHA1:
MBEDTLS_MD_SHA1:"cdc87da223d786df3b45e0bbbc721326d1ee2af806cc315475cc6f0d9c66e1b62371d45ce23
92e1ac92844c310102f156a0d8d52c1f4c40ba3aa65095786cb769757a6563ba958fed0bcc984e8b517a3d5f515b23b8a
41e74aa867693f90dfb061a6e86dfaaee64472c00e5f20945729cbebe77f06ce78e08f4098fba41f9d6193c0317e8b60d4
b6084acb42d29e3808a3bc372d85e331170fcbf7cc72d0b71c296648b3a4d10f416295d0807aa625cab2744fd9ea8fd22
3c42537029828bd16be02546f130fd2e33b936d2676e08aed1b73318b750a0167d0":"dee959c7e06411361420ff8018
5ed57f3e6776af":"9074308fb598e9701b2294388e52f971faac2b60a5145af185df5287b5ed2887e57ce7fd44dc8634e
407c8e0e4360bc226f3ec227f9d9e54638e8d31f5051215df6ebb9c2f9579aa77598a38f914b5b9c1bd83c4e2f9f382a0d
0aa3542ffee65984a601bc69eb28deb27dca12c82c2d4c3f66cd500f1ff2b994d8a4e30cbb33c":0

RSASSA-PSS

Signature Example 1_1 (verify)

pkcs1_rsassa_pss_verify:1024:16:"a56e4a0e701017589a5187dc7ea841d156f2ec0e36ad52a44dfeb1e61f7ad991d8c5
1056ffedb162b4c0f283a12a88a394dff526ab7291cbb307ceabfce0b1dfd5cd9508096d5b2b8b6df5d671ef6377c0921c
b23c270a70e2598e6ff89d19f105acc2d3f0cb35f29280e1386b6f64c4ef22e1e1f20d0ce8cffb2249bd9a2137":16:"0100
01":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"cdc87da223d786df3b45e0bbbc721326d1ee2af806cc315475c
c6f0d9c66e1b62371d45ce2392e1ac92844c310102f156a0d8d52c1f4c40ba3aa65095786cb769757a6563ba958fed0bc
c984e8b517a3d5f515b23b8a41e74aa867693f90dfb061a6e86dfaaee64472c00e5f20945729cbebe77f06ce78e08f4098
fba41f9d6193c0317e8b60d4b6084acb42d29e3808a3bc372d85e331170fcbf7cc72d0b71c296648b3a4d10f416295d0
807aa625cab2744fd9ea8fd223c42537029828bd16be02546f130fd2e33b936d2676e08aed1b73318b750a0167d0":"de
e959c7e06411361420ff80185ed57f3e6776af":"9074308fb598e9701b2294388e52f971faac2b60a5145af185df5287b
5ed2887e57ce7fd44dc8634e407c8e0e4360bc226f3ec227f9d9e54638e8d31f5051215df6ebb9c2f9579aa77598a38f91
4b5b9c1bd83c4e2f9f382a0d0aa3542ffee65984a601bc69eb28deb27dca12c82c2d4c3f66cd500f1ff2b994d8a4e30cbb
33c":0

RSASSA-PSS

Signature Example 1_2

pkcs1_rsassa_pss_sign:1024:16:"e7e8942720a877517273a356053ea2a1bc0c94aa72d55c6e86296b2dfc967948c0a7
2cbccca7eacb35706e09a1df55a1535bd9b3cc34160b3b6dcd3eda8e6443":16:"b69dca1cf7d4d7ec81e75b90fcca874a
bcde123fd2700180aa90479b6e48de8d67ed24f9f19d85ba275874f542cd20dc723e6963364a1f9425452b269a6799fd"
:16:"a56e4a0e701017589a5187dc7ea841d156f2ec0e36ad52a44dfeb1e61f7ad991d8c51056ffedb162b4c0f283a12a88
a394dff526ab7291cbb307ceabfce0b1dfd5cd9508096d5b2b8b6df5d671ef6377c0921cb23c270a70e2598e6ff89d19f1
05acc2d3f0cb35f29280e1386b6f64c4ef22e1e1f20d0ce8cffb2249bd9a2137":16:"010001":MBEDTLS_MD_SHA1:
MBEDTLS_MD_SHA1:"851384cdfe819c22ed6c4ccb30daeb5cf059bc8e1166b7e3530c4c233e2b5f8f71a1cca582d4
3ecc72b1bca16dfc7013226b9e":"ef2869fa40c346cb183dab3d7bffc98fd56df42d":"3ef7f46e831bf92b32274142a585
ffcefbdca7b32ae90d10fb0f0c729984f04ef29a9df0780775ce43739b97838390db0a5505e63de927028d9d29b219ca2c
4517832558a55d694a6d25b9dab66003c4cccd907802193be5170d26147d37b93590241be51c25055f47ef62752cfbe2
1418fafe98c22c4d4d47724fdb5669e843":0

RSASSA-PSS

Signature Example 1_2 (verify)

pkcs1_rsassa_pss_verify:1024:16:"a56e4a0e701017589a5187dc7ea841d156f2ec0e36ad52a44dfeb1e61f7ad991d8c5
1056ffedb162b4c0f283a12a88a394dff526ab7291cbb307ceabfce0b1dfd5cd9508096d5b2b8b6df5d671ef6377c0921c
b23c270a70e2598e6ff89d19f105acc2d3f0cb35f29280e1386b6f64c4ef22e1e1f20d0ce8cffb2249bd9a2137":16:"0100
01":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"851384cdfe819c22ed6c4ccb30daeb5cf059bc8e1166b7e3530
c4c233e2b5f8f71a1cca582d43ecc72b1bca16dfc7013226b9e":"ef2869fa40c346cb183dab3d7bffc98fd56df42d":"3ef
7f46e831bf92b32274142a585ffcefbdca7b32ae90d10fb0f0c729984f04ef29a9df0780775ce43739b97838390db0a550

5e63de927028d9d29b219ca2c4517832558a55d694a6d25b9dab66003c4cccd907802193be5170d26147d37b93590241be51c25055f47ef62752cfbe21418fafe98c22c4d4d47724fdb5669e843":0

RSASSA-PSS
Signature Example 1_3
pkcs1_rsassa_pss_sign:1024:16:"e7e8942720a877517273a356053ea2a1bc0c94aa72d55c6e86296b2dfc967948c0a72cbccca7eacb35706e09a1df55a1535bd9b3cc34160b3b6dcd3eda8e6443":16:"b69dca1cf7d4d7ec81e75b90fcca874abcde123fd2700180aa90479b6e48de8d67ed24f9f19d85ba275874f542cd20dc723e6963364a1f9425452b269a6799fd":16:"a56e4a0e701017589a5187dc7ea841d156f2ec0e36ad52a44dfeb1e61f7ad991d8c51056ffedb162b4c0f283a12a88a394dff526ab7291cbb307ceabfce0b1dfd5cd9508096d5b2b8b6df5d671ef6377c0921cb23c270a70e2598e6ff89d19f105acc2d3f0cb35f29280e1386b6f64c4ef22e1e1f20d0ce8cffb2249bd9a2137":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"a4b159941761c40c6a82f2b80d1b94f5aa2654fd17e12d588864679b54cd04ef8bd03012be8dc37f4b83af7963faff0dfa225477437c48017ff2be8191cf3955fc07356eab3f322f7f620e21d254e5db4324279fe067e0910e2e81ca2cab31c745e67a54058eb50d993cdb9ed0b4d029c06d21a94ca661c3ce27fae1d6cb20f4564d66ce4767583d0e5f060215b59017be85ea848939127bd8c9c4d47b51056c031cf336f17c9980f3b8f5b9b6878e8b797aa43b882684333e17893fe9caa6aa299f7ed1a18ee2c54864b7b2b99b72618fb02574d139ef50f019c9eef416971338e7d470":"710b9c4747d800d4de87f12afdce6df18107cc77":"666026fba71bd3e7cf13157cc2c51a8e4aa684af9778f91849f34335d141c00154c4197621f9624a675b5abc22ee7d5baaffaae1c9baca2cc373b3f33e78e6143c395a91aa7faca664eb733afd14d8827259d99a7550faca501ef2b04e33c23aa51f4b9e8282efdb728cc0ab09405a91607c6369961bc8270d2d4f39fce612b1":0

RSASSA-PSS
Signature Example 1_3 (verify)
pkcs1_rsassa_pss_verify:1024:16:"a56e4a0e701017589a5187dc7ea841d156f2ec0e36ad52a44dfeb1e61f7ad991d8c51056ffedb162b4c0f283a12a88a394dff526ab7291cbb307ceabfce0b1dfd5cd9508096d5b2b8b6df5d671ef6377c0921cb23c270a70e2598e6ff89d19f105acc2d3f0cb35f29280e1386b6f64c4ef22e1e1f20d0ce8cffb2249bd9a2137":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"a4b159941761c40c6a82f2b80d1b94f5aa2654fd17e12d588864679b54cd04ef8bd03012be8dc37f4b83af7963faff0dfa225477437c48017ff2be8191cf3955fc07356eab3f322f7f620e21d254e5db4324279fe067e0910e2e81ca2cab31c745e67a54058eb50d993cdb9ed0b4d029c06d21a94ca661c3ce27fae1d6cb20f4564d66ce4767583d0e5f060215b59017be85ea848939127bd8c9c4d47b51056c031cf336f17c9980f3b8f5b9b6878e8b797aa43b882684333e17893fe9caa6aa299f7ed1a18ee2c54864b7b2b99b72618fb02574d139ef50f019c9eef416971338e7d470":"710b9c4747d800d4de87f12afdce6df18107cc77":"666026fba71bd3e7cf13157cc2c51a8e4aa684af9778f91849f34335d141c00154c4197621f9624a675b5abc22ee7d5baaffaae1c9baca2cc373b3f33e78e6143c395a91aa7faca664eb733afd14d8827259d99a7550faca501ef2b04e33c23aa51f4b9e8282efdb728cc0ab09405a91607c6369961bc8270d2d4f39fce612b1":0

RSASSA-PSS
Signature Example 1_4
pkcs1_rsassa_pss_sign:1024:16:"e7e8942720a877517273a356053ea2a1bc0c94aa72d55c6e86296b2dfc967948c0a72cbccca7eacb35706e09a1df55a1535bd9b3cc34160b3b6dcd3eda8e6443":16:"b69dca1cf7d4d7ec81e75b90fcca874abcde123fd2700180aa90479b6e48de8d67ed24f9f19d85ba275874f542cd20dc723e6963364a1f9425452b269a6799fd":16:"a56e4a0e701017589a5187dc7ea841d156f2ec0e36ad52a44dfeb1e61f7ad991d8c51056ffedb162b4c0f283a12a88a394dff526ab7291cbb307ceabfce0b1dfd5cd9508096d5b2b8b6df5d671ef6377c0921cb23c270a70e2598e6ff89d19f105acc2d3f0cb35f29280e1386b6f64c4ef22e1e1f20d0ce8cffb2249bd9a2137":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"bc656747fa9eafb3f0":"056f00985de14d8ef5cea9e82f8c27bef720335e":"4609793b23e9d09362dc21bb47da0b4f3a7622649a47d464019b9aeafe53359c178c91cd58ba6bcb78be0346a7bc637f4b873d4bab38ee661f199634c547a1ad8442e03da015b136e543f7ab07c0c13e4225b8de8cce25d4f6eb8400f81f7e1833b7ee6e334d370964ca79fdb872b4d75223b5eeb08101591fb532d155a6de87":0

RSASSA-PSS
Signature Example 1_4 (verify)
pkcs1_rsassa_pss_verify:1024:16:"a56e4a0e701017589a5187dc7ea841d156f2ec0e36ad52a44dfeb1e61f7ad991d8c5
1056ffedb162b4c0f283a12a88a394dff526ab7291cbb307ceabfce0b1dfd5cd9508096d5b2b8b6df5d671ef6377c0921c
b23c270a70e2598e6ff89d19f105acc2d3f0cb35f29280e1386b6f64c4ef22e1e1f20d0ce8cffb2249bd9a2137":16:"0100
01":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"bc656747fa9eafb3f0":"056f00985de14d8ef5cea9e82f8c27be
f720335e":"4609793b23e9d09362dc21bb47da0b4f3a7622649a47d464019b9aeafe53359c178c91cd58ba6bcb78be03
46a7bc637f4b873d4bab38ee661f199634c547a1ad8442e03da015b136e543f7ab07c0c13e4225b8de8cce25d4f6eb840
0f81f7e1833b7ee6e334d370964ca79fdb872b4d75223b5eeb08101591fb532d155a6de87":0

RSASSA-PSS Signature Example 1_5
pkcs1_rsassa_pss_sign:1024:16:"e7e8942720a877517273a356053ea2a1bc0c94aa72d55c6e86296b2dfc967948c0a7
2cbccca7eacb35706e09a1df55a1535bd9b3cc34160b3b6dcd3eda8e6443":16:"b69dca1cf7d4d7ec81e75b90fcca874a
bcde123fd2700180aa90479b6e48de8d67ed24f9f19d85ba275874f542cd20dc723e6963364a1f9425452b269a6799fd"
:16:"a56e4a0e701017589a5187dc7ea841d156f2ec0e36ad52a44dfeb1e61f7ad991d8c51056ffedb162b4c0f283a12a88
a394dff526ab7291cbb307ceabfce0b1dfd5cd9508096d5b2b8b6df5d671ef6377c0921cb23c270a70e2598e6ff89d19f1
05acc2d3f0cb35f29280e1386b6f64c4ef22e1e1f20d0ce8cffb2249bd9a2137":16:"010001":MBEDTLS_MD_SHA1:
MBEDTLS_MD_SHA1:"b45581547e5427770c768e8b82b75564e0ea4e9c32594d6bff706544de0a8776c7a80b4576
550eee1b2acabc7e8b7d3ef7bb5b03e462c11047eadd00629ae575480ac1470fe046f13a2bf5af17921dc4b0aa8b02bee6
334911651d7f8525d10f32b51d33be520d3ddf5a709955a3dfe78283b9e0ab54046d150c177f037fdccc5be4ea5f68b5e
5a38c9d7edcccc4975f455a6909b4":"80e70ff86a08de3ec60972b39b4fbfdcea67ae8e":"1d2aad221ca4d31ddf135092
39019398e3d14b32dc34dc5af4aeaea3c095af73479cf0a45e5629635a53a018377615b16cb9b13b3e09d671eb71e387
b8545c5960da5a64776e768e82b2c93583bf104c3fdb23512b7b4e89f633dd0063a530db4524b01c3f384c09310e315a
79dcd3d684022a7f31c865a664e316978b759fad":0

RSASSA-PSS
Signature Example 1_5 (verify)
pkcs1_rsassa_pss_verify:1024:16:"a56e4a0e701017589a5187dc7ea841d156f2ec0e36ad52a44dfeb1e61f7ad991d8c5
1056ffedb162b4c0f283a12a88a394dff526ab7291cbb307ceabfce0b1dfd5cd9508096d5b2b8b6df5d671ef6377c0921c
b23c270a70e2598e6ff89d19f105acc2d3f0cb35f29280e1386b6f64c4ef22e1e1f20d0ce8cffb2249bd9a2137":16:"0100
01":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"b45581547e5427770c768e8b82b75564e0ea4e9c32594d6bff
706544de0a8776c7a80b4576550eee1b2acabc7e8b7d3ef7bb5b03e462c11047eadd00629ae575480ac1470fe046f13a2
bf5af17921dc4b0aa8b02bee6334911651d7f8525d10f32b51d33be520d3ddf5a709955a3dfe78283b9e0ab54046d150c
177f037fdccc5be4ea5f68b5e5a38c9d7edcccc4975f455a6909b4":"80e70ff86a08de3ec60972b39b4fbfdcea67ae8e":"
1d2aad221ca4d31ddf13509239019398e3d14b32dc34dc5af4aeaea3c095af73479cf0a45e5629635a53a018377615b16
cb9b13b3e09d671eb71e387b8545c5960da5a64776e768e82b2c93583bf104c3fdb23512b7b4e89f633dd0063a530db4
524b01c3f384c09310e315a79dcd3d684022a7f31c865a664e316978b759fad":0

RSASSA-PSS
Signature Example 1_6
pkcs1_rsassa_pss_sign:1024:16:"e7e8942720a877517273a356053ea2a1bc0c94aa72d55c6e86296b2dfc967948c0a7
2cbccca7eacb35706e09a1df55a1535bd9b3cc34160b3b6dcd3eda8e6443":16:"b69dca1cf7d4d7ec81e75b90fcca874a
bcde123fd2700180aa90479b6e48de8d67ed24f9f19d85ba275874f542cd20dc723e6963364a1f9425452b269a6799fd"
:16:"a56e4a0e701017589a5187dc7ea841d156f2ec0e36ad52a44dfeb1e61f7ad991d8c51056ffedb162b4c0f283a12a88
a394dff526ab7291cbb307ceabfce0b1dfd5cd9508096d5b2b8b6df5d671ef6377c0921cb23c270a70e2598e6ff89d19f1
05acc2d3f0cb35f29280e1386b6f64c4ef22e1e1f20d0ce8cffb2249bd9a2137":16:"010001":MBEDTLS_MD_SHA1:
MBEDTLS_MD_SHA1:"10aae9a0ab0b595d0841207b700d48d75faedde3b775cd6b4cc88ae06e4694ec74ba18f8520

d4f5ea69cbbe7cc2beba43efdc10215ac4eb32dc302a1f53dc6c4352267e7936cfebf7c8d67035784a3909fa859c7b7b59b8e39c5c2349f1886b705a30267d402f7486ab4f58cad5d69adb17ab8cd0ce1caf5025af4ae24b1fb8794c6070cc09a51e2f9911311e3877d0044c71c57a993395008806b723ac38373d395481818528c1e7053739282053529510e935cd0fa77b8fa53cc2d474bd4fb3cc5c672d6ffdc90a00f9848712c4bcfe46c60573659b11e6457e861f0f604b6138d144f8ce4e2da73":"a8ab69dd801f0074c2a1fc60649836c616d99681":"2a34f6125e1f6b0bf971e84fbd41c632be8f2c2ace7de8b6926e31ff93e9af987fbc06e51e9be14f5198f91f3f953bd67da60a9df59764c3dc0fe08e1cbef0b75f868d10ad3fba749fef59fb6dac46a0d6e504369331586f58e4628f39aa278982543bc0eeb537dc61958019b394fb273f215858a0a01ac4d650b955c67f4c58":0

RSASSA-PSS

Signature Example 1_6 (verify)

pkcs1_rsassa_pss_verify:1024:16:"a56e4a0e701017589a5187dc7ea841d156f2ec0e36ad52a44dfeb1e61f7ad991d8c51056ffedb162b4c0f283a12a88a394dff526ab7291cbb307ceabfce0b1dfd5cd9508096d5b2b8b6df5d671ef6377c0921cb23c270a70e2598e6ff89d19f105acc2d3f0cb35f29280e1386b6f64c4ef22e1e1f20d0ce8cffb2249bd9a2137":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"10aae9a0ab0b595d0841207b700d48d75faedde3b775cd6b4cc88ae06e4694ec74ba18f8520d4f5ea69cbbe7cc2beba43efdc10215ac4eb32dc302a1f53dc6c4352267e7936cfebf7c8d67035784a3909fa859c7b7b59b8e39c5c2349f1886b705a30267d402f7486ab4f58cad5d69adb17ab8cd0ce1caf5025af4ae24b1fb8794c6070cc09a51e2f9911311e3877d0044c71c57a993395008806b723ac38373d395481818528c1e7053739282053529510e935cd0fa77b8fa53cc2d474bd4fb3cc5c672d6ffdc90a00f9848712c4bcfe46c60573659b11e6457e861f0f604b6138d144f8ce4e2da73":"a8ab69dd801f0074c2a1fc60649836c616d99681":"2a34f6125e1f6b0bf971e84fbd41c632be8f2c2ace7de8b6926e31ff93e9af987fbc06e51e9be14f5198f91f3f953bd67da60a9df59764c3dc0fe08e1cbef0b75f868d10ad3fba749fef59fb6dac46a0d6e504369331586f58e4628f39aa278982543bc0eeb537dc61958019b394fb273f215858a0a01ac4d650b955c67f4c58":0

RSASSA-PSS

Signature Example 2_1

pkcs1_rsassa_pss_sign:1025:16:"016601e926a0f8c9e26ecab769ea65a5e7c52cc9e080ef519457c644da6891c5a104d3ea7955929a22e7c68a7af9fcad777c3ccc2b9e3d3650bce404399b7e59d1":16:"014eafa1d4d0184da7e31f877d1281ddda625664869e8379e67ad3b75eae74a580e9827abd6eb7a002cb5411f5266797768fb8e95ae40e3e8a01f35ff89e56c079":16:"01d40c1bcf97a68ae7cdbd8a7bf3e34fa19dcca4ef75a47454375f94514d88fed006fb829f8419ff87d6315da68a1ff3a0938e9abb3464011c303ad99199cf0c7c7a8b477dce829e8844f625b115e5e9c4a59cf8f8113b6834336a2fd2689b472cbb5e5cabe674350c59b6c17e176874fb42f8fc3d176a017edc61fd326c4b33c9":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"daba032066263faedb659848115278a52c44faa3a76f37515ed336321072c40a9d9b53bc05014078adf520875146aae70ff060226dcb7b1f1fc27e9360":"57bf160bcb02bb1dc7280cf0458530b7d2832ff7":"014c5ba5338328ccc6e7a90bf1c0ab3fd606ff4796d3c12e4b639ed9136a5fec6c16d8884bdd99cfdc521456b0742b736868cf90de099adb8d5ffd1deff39ba4007ab746cefdb22d7df0e225f54627dc65466131721b90af445363a8358b9f607642f78fab0ab0f43b7168d64bae70d8827848d8ef1e421c5754ddf42c2589b5b3":0

RSASSA-PSS

Signature Example 2_1 (verify)

pkcs1_rsassa_pss_verify:1025:16:"01d40c1bcf97a68ae7cdbd8a7bf3e34fa19dcca4ef75a47454375f94514d88fed006fb829f8419ff87d6315da68a1ff3a0938e9abb3464011c303ad99199cf0c7c7a8b477dce829e8844f625b115e5e9c4a59cf8f8113b6834336a2fd2689b472cbb5e5cabe674350c59b6c17e176874fb42f8fc3d176a017edc61fd326c4b33c9":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"daba032066263faedb659848115278a52c44faa3a76f375155ed336321072c40a9d9b53bc05014078adf520875146aae70ff060226dcb7b1f1fc27e9360":"57bf160bcb02bb1dc7280cf0458530b7d2832ff7":"014c5ba5338328ccc6e7a90bf1c0ab3fd606ff4796d3c12e4b639ed9136a5fec6c16d8884bdd99cfdc521456b0742b736868cf90de099adb8d5ffd1deff39ba4007ab746cefdb22d7df0e225f54627dc65466131721b90af445363a8358b9f607642f78fab0ab0f43b7168d64bae70d8827848d8ef1e421c5754ddf42c2589b5b3":0

RSASSA-PSS

Signature Example 2_2

pkcs1_rsassa_pss_sign:1025:16:"016601e926a0f8c9e26ecab769ea65a5e7c52cc9e080ef519457c644da6891c5a104d3ea7955929a22e7c68a7af9fcad777c3ccc2b9e3d3650bce404399b7e59d1":16:"014eafa1d4d0184da7e31f877d1281ddda625664869e8379e67ad3b75eae74a580e9827abd6eb7a002cb5411f5266797768fb8e95ae40e3e8a01f35ff89e56c079":16:"01d40c1bcf97a68ae7cdbd8a7bf3e34fa19dcca4ef75a47454375f94514d88fed006fb829f8419ff87d6315da68a1ff3a0938e9abb3464011c303ad99199cf0c7c7a8b477dce829e8844f625b115e5e9c4a59cf8f8113b6834336a2fd2689b472cbb5e5cabe674350c59b6c17e176874fb42f8fc3d176a017edc61fd326c4b33c9":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"e4f8601a8a6da1be34447c0959c058570c3668cfd51dd5f9ccd6ad4411fe8213486d78a6c49f93efc2ca2288cebc2b9b60bd04b1e220d86e3d4848d709d032d1e8c6a070c6af9a499fcf95354b14ba6127c739de1bb0fd16431e46938aec0cf8ad9eb72e832a7035de9b7807bdc0ed8b68eb0f5ac2216be40ce920c0db0eddd3860ed788efaccaca502d8f2bd6d1a7c1f41ff46f1681c8f1f818e9c4f6d91a0c7803ccc63d76a6544d843e084e363b8acc55aa531733edb5dee5b5196e9f03e8b731b3776428d9e457fe3fbcb3db7274442d785890e9cb0854b6444dace791d7273de1889719338a77fe":"7f6dd359e604e60870e898e47b19bf2e5a7b2a90":"010991656cca182b7f29d2dbc007e7ae0fec158eb6759cb9c45c5ff87c7635dd46d150882f4de1e9ae65e7f7d9018f6836954a47c0a81a8a6b6f83f2944d6081b1aa7c759b254b2c34b691da67cc0226e20b2f18b42212761dcd4b908a62b371b5918c5742af4b537e296917674fb9141947616 21cc19a41f6fb953fbcbb649dea":0

RSASSA-PSS

Signature Example 2_2 (verify)

pkcs1_rsassa_pss_verify:1025:16:"01d40c1bcf97a68ae7cdbd8a7bf3e34fa19dcca4ef75a47454375f94514d88fed006fb829f8419ff87d6315da68a1ff3a0938e9abb3464011c303ad99199cf0c7c7a8b477dce829e8844f625b115e5e9c4a59cf8f8113b6834336a2fd2689b472cbb5e5cabe674350c59b6c17e176874fb42f8fc3d176a017edc61fd326c4b33c9":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"e4f8601a8a6da1be34447c0959c058570c3668cfd51dd5f9ccd6ad4411fe8213486d78a6c49f93efc2ca2288cebc2b9b60bd04b1e220d86e3d4848d709d032d1e8c6a070c6af9a499fcf95354b14ba6127c739de1bb0fd16431e46938aec0cf8ad9eb72e832a7035de9b7807bdc0ed8b68eb0f5ac2216be40ce920c0db0eddd3860ed788efaccaca502d8f2bd6d1a7c1f41ff46f1681c8f1f818e9c4f6d91a0c7803ccc63d76a6544d843e084e363b8acc55aa531733edb5dee5b5196e9f03e8b731b3776428d9e457fe3fbcb3db7274442d785890e9cb0854b6444dace791d7273de1889719338a77fe":"7f6dd359e604e60870e898e47b19bf2e5a7b2a90":"010991656cca182b7f29d2dbc007e7ae0fec158eb6759cb9c45c5ff87c7635dd46d150882f4de1e9ae65e7f7d9018f6836954a47c0a81a8a6b6f83f2944d6081b1aa7c759b254b2c34b691da67cc0226e20b2f18b42212761dcd4b908a62b371b5918c5742af4b537e296917674fb914194761621cc19a41f6fb953fbcbb649dea":0

RSASSA-PSS

Signature Example 2_3

pkcs1_rsassa_pss_sign:1025:16:"016601e926a0f8c9e26ecab769ea65a5e7c52cc9e080ef519457c644da6891c5a104d3ea7955929a22e7c68a7af9fcad777c3ccc2b9e3d3650bce404399b7e59d1":16:"014eafa1d4d0184da7e31f877d1281ddda625664869e8379e67ad3b75eae74a580e9827abd6eb7a002cb5411f5266797768fb8e95ae40e3e8a01f35ff89e56c079":16:"01d40c1bcf97a68ae7cdbd8a7bf3e34fa19dcca4ef75a47454375f94514d88fed006fb829f8419ff87d6315da68a1ff3a0938e9abb3464011c303ad99199cf0c7c7a8b477dce829e8844f625b115e5e9c4a59cf8f8113b6834336a2fd2689b472cbb5e5cabe674350c59b6c17e176874fb42f8fc3d176a017edc61fd326c4b33c9":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"52a1d96c8ac39e41e455809801b927a5b445c10d902a0dcd3850d22a66d2bb0703e67d5867114595aabf5a7aeb5a8f87034bbb30e13cfd4817a9be76230023606d0286a3faf8a4d22b728ec518079f9e64526e3a0cc7941aa338c437997c680ccac67c66bfa1":"fca862068bce2246724b708a0519da17e648688c":"007f0030018f53cdc71f23d03659fde54d4241f758a750b42f185f87578520c30742afd84359b6e6e8d3ed959dc6fe486bedc8e2cf001f63a7abe16256a1b84df0d249fc05d3194ce5f0912742dbbf80dd174f6c51f6bad7f16cf3364eba095a06267dc3793803ac7526aebe0a475d38b8c2247ab51c4898df7047dc6adf52c6c4":0

RSASSA-PSS
Signature Example 2_3 (verify)
pkcs1_rsassa_pss_verify:1025:16:"01d40c1bcf97a68ae7cdbd8a7bf3e34fa19dcca4ef75a47454375f94514d88fed006fb829f8419ff87d6315da68a1ff3a0938e9abb3464011c303ad99199cf0c7c7a8b477dce829e8844f625b115e5e9c4a59cf8f8113b6834336a2fd2689b472cbb5e5cabe674350c59b6c17e176874fb42f8fc3d176a017edc61fd326c4b33c9":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"52a1d96c8ac39e41e455809801b927a5b445c10d902a0dcd3850d22a66d2bb0703e67d5867114595aabf5a7aeb5a8f87034bbb30e13cfd4817a9be76230023606d0286a3faf8a4d22b728ec518079f9e64526e3a0cc7941aa338c437997c680ccac67c66bfa1":"fca862068bce2246724b708a0519da17e648688c":"007f0030018f53cdc71f23d03659fde54d4241f758a750b42f185f87578520c30742afd84359b6e6e8d3ed959dc6fe486bedc8e2cf001f63a7abe16256a1b84df0d249fc05d3194ce5f0912742dbbf80dd174f6c51f6bad7f16cf3364eba095a06267dc3793803ac7526aebe0a475d38b8c2247ab51c4898df7047dc6adf52c6c4":0

RSASSA-PSS
Signature Example 2_4
pkcs1_rsassa_pss_sign:1025:16:"016601e926a0f8c9e26ecab769ea65a5e7c52cc9e080ef519457c644da6891c5a104d3ea7955929a22e7c68a7af9fcad777c3ccc2b9e3d3650bce404399b7e59d1":16:"014eafa1d4d0184da7e31f877d1281ddda625664869e8379e67ad3b75eae74a580e9827abd6eb7a002cb5411f5266797768fb8e95ae40e3e8a01f35ff89e56c079":16:"01d40c1bcf97a68ae7cdbd8a7bf3e34fa19dcca4ef75a47454375f94514d88fed006fb829f8419ff87d6315da68a1ff3a0938e9abb3464011c303ad99199cf0c7c7a8b477dce829e8844f625b115e5e9c4a59cf8f8113b6834336a2fd2689b472cbb5e5cabe674350c59b6c17e176874fb42f8fc3d176a017edc61fd326c4b33c9":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"a7182c83ac18be6570a106aa9d5c4e3dbbd4afaeb0c60c4a23e1969d79ff":"8070ef2de945c02387684ba0d33096732235d440":"009cd2f4edbe23e12346ae8c76dd9ad3230a62076141f16c152ba18513a48ef6f010e0e37fd3df10a1ec629a0cb5a3b5d2893007298c30936a95903b6ba85555d9ec3673a06108fd62a2fda56d1ce2e85c4db6b24a81ca3b496c36d4fd06eb7c9166d8e94877c42bea622b3bfe9251fdc21d8d5371badad78a488214796335b40b":0

RSASSA-PSS
Signature Example 2_4 (verify)
pkcs1_rsassa_pss_verify:1025:16:"01d40c1bcf97a68ae7cdbd8a7bf3e34fa19dcca4ef75a47454375f94514d88fed006fb829f8419ff87d6315da68a1ff3a0938e9abb3464011c303ad99199cf0c7c7a8b477dce829e8844f625b115e5e9c4a59cf8f8113b6834336a2fd2689b472cbb5e5cabe674350c59b6c17e176874fb42f8fc3d176a017edc61fd326c4b33c9":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"a7182c83ac18be6570a106aa9d5c4e3dbbd4afaeb0c60c4a23e1969d79ff":"8070ef2de945c02387684ba0d33096732235d440":"009cd2f4edbe23e12346ae8c76dd9ad3230a62076141f16c152ba18513a48ef6f010e0e37fd3df10a1ec629a0cb5a3b5d2893007298c30936a95903b6ba85555d9ec3673a06108fd62a2fda56d1ce2e85c4db6b24a81ca3b496c36d4fd06eb7c9166d8e94877c42bea622b3bfe9251fdc21d8d5371badad78a488214796335b40b":0

RSASSA-PSS Signature Example 2_5
pkcs1_rsassa_pss_sign:1025:16:"016601e926a0f8c9e26ecab769ea65a5e7c52cc9e080ef519457c644da6891c5a104d3ea7955929a22e7c68a7af9fcad777c3ccc2b9e3d3650bce404399b7e59d1":16:"014eafa1d4d0184da7e31f877d1281ddda625664869e8379e67ad3b75eae74a580e9827abd6eb7a002cb5411f5266797768fb8e95ae40e3e8a01f35ff89e56c079":16:"01d40c1bcf97a68ae7cdbd8a7bf3e34fa19dcca4ef75a47454375f94514d88fed006fb829f8419ff87d6315da68a1ff3a0938e9abb3464011c303ad99199cf0c7c7a8b477dce829e8844f625b115e5e9c4a59cf8f8113b6834336a2fd2689b472cbb5e5cabe674350c59b6c17e176874fb42f8fc3d176a017edc61fd326c4b33c9":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"86a83d4a72ee932a4f5630af6579a386b78fe88999e0abd2d49034a4bfc854dd94f1094e2e8cd7a179d19588e4aefc1b1bd25e95e3dd461f":"17639a4e88d722c4fca24d079a8b29c32433b0c9":"00ec430824931ebd3baa43034dae98ba646b8c36013d1671c3cf1cf8260c374b19f8e1cc8d965012405e7e9bf7378612dfcc85fce12

cda11f950bd0ba8876740436c1d2595a64a1b32efcfb74a21c873b3cc33aaf4e3dc3953de67f0674c0453b4fd9f604406d441b816098cb106fe3472bc251f815f59db2e4378a3addc181ecf":0

RSASSA-PSS
Signature Example 2_5 (verify)
pkcs1_rsassa_pss_verify:1025:16:"01d40c1bcf97a68ae7cdbd8a7bf3e34fa19dcca4ef75a47454375f94514d88fed006fb829f8419ff87d6315da68a1ff3a0938e9abb3464011c303ad99199cf0c7c7a8b477dce829e8844f625b115e5e9c4a59cf8f8113b6834336a2fd2689b472cbb5e5cabe674350c59b6c17e176874fb42f8fc3d176a017edc61fd326c4b33c9":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"86a83d4a72ee932a4f5630af6579a386b78fe88999e0abd2d49034a4bfc854dd94f1094e2e8cd7a179d19588e4aefc1b1bd25e95e3dd461f":"17639a4e88d722c4fca24d079a8b29c32433b0c9":"00ec430824931ebd3baa43034dae98ba646b8c36013d1671c3cf1cf8260c374b19f8e1cc8d965012405e7e9bf7378612dfcc85fce12cda11f950bd0ba8876740436c1d2595a64a1b32efcfb74a21c873b3cc33aaf4e3dc3953de67f0674c0453b4fd9f604406d441b816098cb106fe3472bc251f815f59db2e4378a3addc181ecf":0

RSASSA-PSS Signature Example 2_6
pkcs1_rsassa_pss_sign:1025:16:"016601e926a0f8c9e26ecab769ea65a5e7c52cc9e080ef519457c644da6891c5a104d3ea7955929a22e7c68a7af9fcad777c3ccc2b9e3d3650bce404399b7e59d1":16:"014eafa1d4d0184da7e31f877d1281ddda625664869e8379e67ad3b75eae74a580e9827abd6eb7a002cb5411f5266797768fb8e95ae40e3e8a01f35ff89e56c079":16:"01d40c1bcf97a68ae7cdbd8a7bf3e34fa19dcca4ef75a47454375f94514d88fed006fb829f8419ff87d6315da68a1ff3a0938e9abb3464011c303ad99199cf0c7c7a8b477dce829e8844f625b115e5e9c4a59cf8f8113b6834336a2fd2689b472cbb5e5cabe674350c59b6c17e176874fb42f8fc3d176a017edc61fd326c4b33c9":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"049f9154d871ac4a7c7ab45325ba7545a1ed08f70525b2667cf1":"37810def1055ed922b063df798de5d0aabf886ee":"00475b1648f814a8dc0abdc37b5527f543b666bb6e39d30e5b49d3b876dccc58eac14e32a2d55c2616014456ad2f246fc8e3d560da3ddf379a1c0bd200f10221df078c219a151bc8d4ec9d2fc2564467811014ef15d8ea01c2ebbff8c2c8efab38096e55fcbe3285c7aa558851254faffa92c1c72b78758663ef4582843139d7a6":0

RSASSA-PSS
Signature Example 2_6 (verify)
pkcs1_rsassa_pss_verify:1025:16:"01d40c1bcf97a68ae7cdbd8a7bf3e34fa19dcca4ef75a47454375f94514d88fed006fb829f8419ff87d6315da68a1ff3a0938e9abb3464011c303ad99199cf0c7c7a8b477dce829e8844f625b115e5e9c4a59cf8f8113b6834336a2fd2689b472cbb5e5cabe674350c59b6c17e176874fb42f8fc3d176a017edc61fd326c4b33c9":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"049f9154d871ac4a7c7ab45325ba7545a1ed08f70525b2667cf1":"37810def1055ed922b063df798de5d0aabf886ee":"00475b1648f814a8dc0abdc37b5527f543b666bb6e39d30e5b49d3b876dccc58eac14e32a2d55c2616014456ad2f246fc8e3d560da3ddf379a1c0bd200f10221df078c219a151bc8d4ec9d2fc2564467811014ef15d8ea01c2ebbff8c2c8efab38096e55fcbe3285c7aa558851254faffa92c1c72b78758663ef4582843139d7a6":0

RSASSA-PSS
Signature Example 3_1
pkcs1_rsassa_pss_sign:1026:16:"01bd36e18ece4b0fdb2e9c9d548bd1a7d6e2c21c6fdc35074a1d05b1c6c8b3d558ea2639c9a9a421680169317252558bd148ad215aac550e2dcf12a82d0ebfe853":16:"01b1b656ad86d8e19d5dc86292b3a192fdf6e0dd37877bad14822fa00190cab265f90d3f02057b6f54d6ecb14491e5adeacebc48bf0ebd2a2ad26d402e54f61651":16:"02f246ef451ed3eebb9a310200cc25859c048e4be798302991112eb68ce6db674e280da21feded1ae74880ca522b18db249385012827c515f0e466a1ffa691d98170574e9d0eadb087586ca48933da3cc953d95bd0ed50de10ddcb6736107d6c831c7f663e833ca4c097e700ce0fb945f88fb85fe8e5a773172565b914a471a443":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"594b37333bbb2c84524a87c1a01f75fcec0e3256f108e38dca36d70d0057":"f31ad6c8cf89df78ed77feacbcc2f8b0a8e4cfaa":"0088b135fb1794b6b96c4a3e678197f8cac52b64b2fe907d6f27de761124964a99a01a882740ecfaed6c01a47464bb05182313c01338a8cd097214cd68ca103bd57d3bc9e816213e61d784f182467

abf8a01cf253e99a156eaa8e3e1f90e3c6e4e3aa2d83ed0345b89fafc9c26077c14b6ac51454fa26e446e3a2f153b2b16797f":0

RSASSA-PSS
Signature Example 3_1 (verify)
pkcs1_rsassa_pss_verify:1026:16:"02f246ef451ed3eebb9a310200cc25859c048e4be798302991112eb68ce6db674e280da21feded1ae74880ca522b18db249385012827c515f0e466a1ffa691d98170574e9d0eadb087586ca48933da3cc953d95bd0ed50de10ddcb6736107d6c831c7f663e833ca4c097e700ce0fb945f88fb85fe8e5a773172565b914a471a443":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"594b37333bbb2c84524a87c1a01f75fcec0e3256f108e38dca36d70d0057":"f31ad6c8cf89df78ed77feacbcc2f8b0a8e4cfaa":"0088b135fb1794b6b96c4a3e678197f8cac52b64b2fe907d6f27de761124964a99a01a882740ecfaed6c01a47464bb05182313c01338a8cd097214cd68ca103bd57d3bc9e816213e61d784f182467abf8a01cf253e99a156eaa8e3e1f90e3c6e4e3aa2d83ed0345b89fafc9c26077c14b6ac51454fa26e446e3a2f153b2b16797f":0

RSASSA-PSS
Signature Example 3_2
pkcs1_rsassa_pss_sign:1026:16:"01bd36e18ece4b0fdb2e9c9d548bd1a7d6e2c21c6fdc35074a1d05b1c6c8b3d558ea2639c9a9a4216801693172525 58bd148ad215aac550e2dcf12a82d0ebfe853":16:"01b1b656ad86d8e19d5dc86292b3a192fdf6e0dd37877bad14822fa00190cab265f90d3f02057b6f54d6ecb14491e5adeacebc48bf0ebd2a2ad26d402e54f61651":16:"02f246ef451ed3eebb9a310200cc25859c048e4be798302991112eb68ce6db674e280da21feded1ae74880ca522b18db249385012827c515f0e466a1ffa691d98170574e9d0eadb087586ca48933da3cc953d95bd0ed50de10ddcb6736107d6c831c7f663e833ca4c097e700ce0fb945f88fb85fe8e5a773172565b914a471a443":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"8b769528884a0d1ffd090cf102993e796dadcfbddd38e44ff6324ca451":"fcf9f0e1f199a3d1d0da681c5b8606fc642939f7":"02a5f0a858a0864a4f65017a7d69454f3f973a2999839b7bbc48bf78641169179556f595fa41f6ff18e286c2783079bc0910ee9cc34f49ba681124f923dfa88f426141a368a5f5a930c628c2c3c200e18a7644721a0cbec6dd3f6279bde3e8f2be5e2d4ee56f97e7ceaf33054be7042bd91a63bb09f897bd41e81197dee99b11af":0

RSASSA-PSS
Signature Example 3_2 (verify)
pkcs1_rsassa_pss_verify:1026:16:"02f246ef451ed3eebb9a310200cc25859c048e4be798302991112eb68ce6db674e280da21feded1ae74880ca522b18db249385012827c515f0e466a1ffa691d98170574e9d0eadb087586ca48933da3cc953d95bd0ed50de10ddcb6736107d6c831c7f663e833ca4c097e700ce0fb945f88fb85fe8e5a773172565b914a471a443":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"8b769528884a0d1ffd090cf102993e796dadcfbddd38e44ff6324ca451":"fcf9f0e1f199a3d1d0da681c5b8606fc642939f7":"02a5f0a858a0864a4f65017a7d69454f3f973a2999839b7bbc48bf78641169179556f595fa41f6ff18e286c2783079bc0910ee9cc34f49ba681124f923dfa88f426141a368a5f5a930c628c2c3c200e18a7644721a0cbec6dd3f6279bde3e8f2be5e2d4ee56f97e7ceaf33054be7042bd91a63bb09f897bd41e81197dee99b11af":0

RSASSA-PSS
Signature Example 3_3
pkcs1_rsassa_pss_sign:1026:16:"01bd36e18ece4b0fdb2e9c9d548bd1a7d6e2c21c6fdc35074a1d05b1c6c8b3d558ea2639c9a9a4216801693172525 58bd148ad215aac550e2dcf12a82d0ebfe853":16:"01b1b656ad86d8e19d5dc86292b3a192fdf6e0dd37877bad14822fa00190cab265f90d3f02057b6f54d6ecb14491e5adeacebc48bf0ebd2a2ad26d402e54f61651":16:"02f246ef451ed3eebb9a310200cc25859c048e4be798302991112eb68ce6db674e280da21feded1ae74880ca522b18db249385012827c515f0e466a1ffa691d98170574e9d0eadb087586ca48933da3cc953d95bd0ed50de10ddcb6736107d6c831c7f663e833ca4c097e700ce0fb945f88fb85fe8e5a773172565b914a471a443":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"1abdba489c5ada2f995ed16f19d5a94d9e6ec34a8d84f84557d26e5ef9b02b22887

e3f9a4b690ad1149209c20c61431f0c017c36c2657b35d7b07d3f5ad8708507a9c1b831df835a56f831071814ea5d3d8
d8f6ade40cba38b42db7a2d3d7a29c8f0a79a7838cf58a9757fa2fe4c40df9baa193bfc6f92b123ad57b07ace3e6ac068c9
f106afd9eeb03b4f37c25dbfbcfb3071f6f9771766d072f3bb070af6605532973ae25051":"986e7c43dbb671bd41b9a7f
4b6afc80e805f2423":"0244bcd1c8c16955736c803be401272e18cb990811b14f72db964124d5fa760649cbb57afb875
5dbb62bf51f466cf23a0a1607576e983d778fceffa92df7548aea8ea4ecad2c29dd9f95bc07fe91ecf8bee255bfe8762fd76
90aa9bfa4fa0849ef728c2c42c4532364522df2ab7f9f8a03b63f7a499175828668f5ef5a29e3802c":0

RSASSA-PSS
Signature Example 3_3 (verify)
pkcs1_rsassa_pss_verify:1026:16:"02f246ef451ed3eebb9a310200cc25859c048e4be798302991112eb68ce6db674e2
80da21feded1ae74880ca522b18db249385012827c515f0e466a1ffa691d98170574e9d0eadb087586ca48933da3cc953
d95bd0ed50de10ddcb6736107d6c831c7f663e833ca4c097e700ce0fb945f88fb85fe8e5a773172565b914a471a443":1
6:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"1abdba489c5ada2f995ed16f19d5a94d9e6ec34a8d84f
84557d26e5ef9b02b22887e3f9a4b690ad1149209c20c61431f0c017c36c2657b35d7b07d3f5ad8708507a9c1b831df8
35a56f831071814ea5d3d8d8f6ade40cba38b42db7a2d3d7a29c8f0a79a7838cf58a9757fa2fe4c40df9baa193bfc6f92b
123ad57b07ace3e6ac068c9f106afd9eeb03b4f37c25dbfbcfb3071f6f9771766d072f3bb070af6605532973ae25051":"9
86e7c43dbb671bd41b9a7f4b6afc80e805f2423":"0244bcd1c8c16955736c803be401272e18cb990811b14f72db96412
4d5fa760649cbb57afb8755dbb62bf51f466cf23a0a1607576e983d778fceffa92df7548aea8ea4ecad2c29dd9f95bc07fe
91ecf8bee255bfe8762fd7690aa9bfa4fa0849ef728c2c42c4532364522df2ab7f9f8a03b63f7a499175828668f5ef5a29e
3802c":0

RSASSA-PSS
Signature Example 3_4
pkcs1_rsassa_pss_sign:1026:16:"01bd36e18ece4b0fdb2e9c9d548bd1a7d6e2c21c6fdc35074a1d05b1c6c8b3d558ea2
639c9a9a4216801693172525 58bd148ad215aac550e2dcf12a82d0ebfe853":16:"01b1b656ad86d8e19d5dc86292b3a1
92fdf6e0dd37877bad14822fa00190cab265f90d3f02057b6f54d6ecb14491e5adeacebc48bf0ebd2a2ad26d402e54f616
51":16:"02f246ef451ed3eebb9a310200cc25859c048e4be798302991112eb68ce6db674e280da21feded1ae74880ca52
2b18db249385012827c515f0e466a1ffa691d98170574e9d0eadb087586ca48933da3cc953d95bd0ed50de10ddcb6736
107d6c831c7f663e833ca4c097e700ce0fb945f88fb85fe8e5a773172565b914a471a443":16:"010001":MBEDTLS_M
D_SHA1:MBEDTLS_MD_SHA1:"8fb431f5ee792b6c2ac7db53cc428655aeb32d03f4e889c5c25de683c461b53acf8
9f9f8d3aabdf6b9f0c2a1de12e15b49edb3919a652fe9491c25a7fce1f722c2543608b69dc375ec":"f8312d9c8eea13ec0
a4c7b98120c87509087c478":"0196f12a005b98129c8df13c4cb16f8aa887d3c40d96df3a88e7532ef39cd992f273abc3
70bc1be6f097cfebbf0118fd9ef4b927155f3df22b904d90702d1f7ba7a52bed8b8942f412cd7bd676c9d18e170391dcd
345c06a730964b3f30bcce0bb20ba106f9ab0eeb39cf8a6607f75c0347f0af79f16afa081d2c92d1ee6f836b8":0

RSASSA-PSS
Signature Example 3_4 (verify)
pkcs1_rsassa_pss_verify:1026:16:"02f246ef451ed3eebb9a310200cc25859c048e4be798302991112eb68ce6db674e2
80da21feded1ae74880ca522b18db249385012827c515f0e466a1ffa691d98170574e9d0eadb087586ca48933da3cc953
d95bd0ed50de10ddcb6736107d6c831c7f663e833ca4c097e700ce0fb945f88fb85fe8e5a773172565b914a471a443":1
6:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"8fb431f5ee792b6c2ac7db53cc428655aeb32d03f4e8
89c5c25de683c461b53acf89f9f8d3aabdf6b9f0c2a1de12e15b49edb3919a652fe9491c25a7fce1f722c2543608b69dc3
75ec":"f8312d9c8eea13ec0a4c7b98120c87509087c478":"0196f12a005b98129c8df13c4cb16f8aa887d3c40d96df3a8
8e7532ef39cd992f273abc370bc1be6f097cfebbf0118fd9ef4b927155f3df22b904d90702d1f7ba7a52bed8b8942f412c
d7bd676c9d18e170391dcd345c06a730964b3f30bcce0bb20ba106f9ab0eeb39cf8a6607f75c0347f0af79f16afa081d2c
92d1ee6f836b8":0

RSASSA-PSS

Signature Example 3_5

pkcs1_rsassa_pss_sign:1026:16:"01bd36e18ece4b0fdb2e9c9d548bd1a7d6e2c21c6fdc35074a1d05b1c6c8b3d558ea2639c9a9a421680169317252558bd148ad215aac550e2dcf12a82d0ebfe853":16:"01b1b656ad86d8e19d5dc86292b3a192fdf6e0dd37877bad14822fa00190cab265f90d3f02057b6f54d6ecb14491e5adeacebc48bf0ebd2a2ad26d402e54f61651":16:"02f246ef451ed3eebb9a310200cc25859c048e4be798302991112eb68ce6db674e280da21feded1ae74880ca522b18db249385012827c515f0e466a1ffa691d98170574e9d0eadb087586ca48933da3cc953d95bd0ed50de10ddcb6736107d6c831c7f663e833ca4c097e700ce0fb945f88fb85fe8e5a773172565b914a471a443":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"fef4161dfaaf9c5295051dfc1ff3810c8c9ec2e866f7075422c8ec4216a9c4ff49427d483cae10c8534a41b2fd15fee06960ec6fb3f7a7e94a2f8a2e3e43dc4a40576c3097ac953b1de86f0b4ed36d644f23ae14425529622464ca0cbf0b1741347238157fab59e4de5524096d62baec63ac64":"50327efec6292f98019fc67a2a6638563e9b6e2d":"021eca3ab4892264ec22411a752d92221076d4e01c0e6f0dde9afd26ba5acf6d739ef987545d16683e5674c9e70f1de649d7e61d48d0caeb4fb4d8b24fba84a6e3108fee7d0705973266ac524b4ad280f7ae17dc59d96d3351586b5a3bdb895d1e1f7820ac6135d8753480998382ba32b7349559608c38745290a85ef4e9f9bd83":0

RSASSA-PSS

Signature Example 3_5 (verify)

pkcs1_rsassa_pss_verify:1026:16:"02f246ef451ed3eebb9a310200cc25859c048e4be798302991112eb68ce6db674e280da21feded1ae74880ca522b18db249385012827c515f0e466a1ffa691d98170574e9d0eadb087586ca48933da3cc953d95bd0ed50de10ddcb6736107d6c831c7f663e833ca4c097e700ce0fb945f88fb85fe8e5a773172565b914a471a443":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"fef4161dfaaf9c5295051dfc1ff3810c8c9ec2e866f7075422c8ec4216a9c4ff49427d483cae10c8534a41b2fd15fee06960ec6fb3f7a7e94a2f8a2e3e43dc4a40576c3097ac953b1de86f0b4ed36d644f23ae14425529622464ca0cbf0b1741347238157fab59e4de5524096d62baec63ac64":"50327efec6292f98019fc67a2a6638563e9b6e2d":"021eca3ab4892264ec22411a752d92221076d4e01c0e6f0dde9afd26ba5acf6d739ef987545d16683e5674c9e70f1de649d7e61d48d0caeb4fb4d8b24fba84a6e3108fee7d0705973266ac524b4ad280f7ae17dc59d96d3351586b5a3bdb895d1e1f7820ac6135d8753480998382ba32b7349559608c38745290a85ef4e9f9bd83":0

RSASSA-PSS

Signature Example 3_6

pkcs1_rsassa_pss_sign:1026:16:"01bd36e18ece4b0fdb2e9c9d548bd1a7d6e2c21c6fdc35074a1d05b1c6c8b3d558ea2639c9a9a421680169317252558bd148ad215aac550e2dcf12a82d0ebfe853":16:"01b1b656ad86d8e19d5dc86292b3a192fdf6e0dd37877bad14822fa00190cab265f90d3f02057b6f54d6ecb14491e5adeacebc48bf0ebd2a2ad26d402e54f61651":16:"02f246ef451ed3eebb9a310200cc25859c048e4be798302991112eb68ce6db674e280da21feded1ae74880ca522b18db249385012827c515f0e466a1ffa691d98170574e9d0eadb087586ca48933da3cc953d95bd0ed50de10ddcb6736107d6c831c7f663e833ca4c097e700ce0fb945f88fb85fe8e5a773172565b914a471a443":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"efd237bb098a443aeeb2bf6c3f8c81b8c01b7fcb3feb":"b0de3fc25b65f5af96b1d5cc3b27d0c6053087b3":"012fafec862f56e9e92f60ab0c77824f4299a0ca734ed26e0644d5d222c7f0bde03964f8e70a5cb65ed44e44d56ae0edf1ff86ca032cc5dd4404dbb76ab854586c44eed8336d08d457ce6c03693b45c0f1efef93624b95b8ec169c616d20e5538ebc0b6737a6f82b4bc0570924fc6b35759a3348426279f8b3d7744e2d222426ce":0

RSASSA-PSS

Signature Example 3_6 (verify)

pkcs1_rsassa_pss_verify:1026:16:"02f246ef451ed3eebb9a310200cc25859c048e4be798302991112eb68ce6db674e280da21feded1ae74880ca522b18db249385012827c515f0e466a1ffa691d98170574e9d0eadb087586ca48933da3cc953d95bd0ed50de10ddcb6736107d6c831c7f663e833ca4c097e700ce0fb945f88fb85fe8e5a773172565b914a471a443":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"efd237bb098a443aeeb2bf6c3f8c81b8c01b7fcb3feb":"b0de3fc25b65f5af96b1d5cc3b27d0c6053087b3":"012fafec862f56e9e92f60ab0c77824f4299a0ca734ed26e0644d5d222c7f0bde03964f8e70a5cb65ed44e44d56ae0edf1ff86ca032cc5dd4404dbb76ab854586c44eed8336d08d457ce6c03

693b45c0f1efef93624b95b8ec169c616d20e5538ebc0b6737a6f82b4bc0570924fc6b35759a3348426279f8b3d7744e2d222426ce":0

RSASSA-PSS
Signature Example 4_1
pkcs1_rsassa_pss_sign:1027:16:"029232336d2838945dba9dd7723f4e624a05f7375b927a87abe6a893a1658fd49f47f6c7b0fa596c65fa68a23f0ab432962d18d4343bd6fd671a5ea8d148413995":16:"020ef5efe7c5394aed2272f7e81a74f4c02d145894cb1b3cab23a9a0710a2afc7e3329acbb743d01f680c4d02afb4c8fde7e20930811bb2b995788b5e872c20bb1":16:"054adb7886447efe6f57e0368f06cf52b0a3370760d161cef126b91be7f89c421b62a6ec1da3c311d75ed50e0ab5fff3fd338acc3aa8a4e77ee26369acb81ba900fa83f5300cf9bb6c53ad1dc8a178b815db4235a9a9da0c06de4e615ea1277ce559e9c108de58c14a81aa77f5a6f8d1335494498848c8b95940740be7bf7c3705":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"9fb03b827c8217d9":"ed7c98c95f30974fbe4fbddcf0f28d6021c0e91d":"0323d5b7bf20ba4539289ae452ae4297080feff4518423ff4811a817837e7d82f1836cdfab54514ff0887bddeebf40bf99b047abc3ecfa6a37a3ef00f4a0c4a88aae0904b745c846c4107e8797723e8ac810d9e3d95dfa30ff4966f4d75d13768d20857f2b1406f264cfe75e27d7652f4b5ed3575f28a702f8c4ed9cf9b2d44948":0

RSASSA-PSS
Signature Example 4_1 (verify)
pkcs1_rsassa_pss_verify:1027:16:"054adb7886447efe6f57e0368f06cf52b0a3370760d161cef126b91be7f89c421b62a6ec1da3c311d75ed50e0ab5fff3fd338acc3aa8a4e77ee26369acb81ba900fa83f5300cf9bb6c53ad1dc8a178b815db4235a9a9da0c06de4e615ea1277ce559e9c108de58c14a81aa77f5a6f8d1335494498848c8b95940740be7bf7c3705":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"9fb03b827c8217d9":"ed7c98c95f30974fbe4fbddcf0f28d6021c0e91d":"0323d5b7bf20ba4539289ae452ae4297080feff4518423ff4811a817837e7d82f1836cdfab54514ff0887bddeebf40bf99b047abc3ecfa6a37a3ef00f4a0c4a88aae0904b745c846c4107e8797723e8ac810d9e3d95dfa30ff4966f4d75d13768d20857f2b1406f264cfe75e27d7652f4b5ed3575f28a702f8c4ed9cf9b2d44948":0

RSASSA-PSS Signature Example 4_2
pkcs1_rsassa_pss_sign:1027:16:"029232336d2838945dba9dd7723f4e624a05f7375b927a87abe6a893a1658fd49f47f6c7b0fa596c65fa68a23f0ab432962d18d4343bd6fd671a5ea8d148413995":16:"020ef5efe7c5394aed2272f7e81a74f4c02d145894cb1b3cab23a9a0710a2afc7e3329acbb743d01f680c4d02afb4c8fde7e20930811bb2b995788b5e872c20bb1":16:"054adb7886447efe6f57e0368f06cf52b0a3370760d161cef126b91be7f89c421b62a6ec1da3c311d75ed50e0ab5fff3fd338acc3aa8a4e77ee26369acb81ba900fa83f5300cf9bb6c53ad1dc8a178b815db4235a9a9da0c06de4e615ea1277ce559e9c108de58c14a81aa77f5a6f8d1335494498848c8b95940740be7bf7c3705":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"0ca2ad77797ece86de5bf768750ddb5ed6a3116ad99bbd17edf7f782f0db1cd05b0f677468c5ea420dc116b10e80d110de2b0461ea14a38be68620392e7e893cb4ea9393fb886c20ff790642305bf302003892e54df9f667509dc53920df583f50a3dd61abb6fab75d600377e383e6aca6710eeea27156e06752c94ce25ae99fcbf8592dbe2d7e27453cb44de07100ebb1a2a19811a478adbeab270f94e8fe369d90b3ca612f9f":"22d71d54363a4217aa55113f059b3384e3e57e44":"049d0185845a264d28feb1e69edaec090609e8e46d93abb38371ce51f4aa65a599bdaaa81d24fba66a08a116cb644f3f1e653d95c89db8bbd5daac2709c8984000178410a7c6aa8667ddc38c741f710ec8665aa9052be929d4e3b16782c1662114c5414bb0353455c392fc28f3db59054b5f365c49e1d156f876ee10cb4fd70598":0

RSASSA-PSS
Signature Example 4_2 (verify)
pkcs1_rsassa_pss_verify:1027:16:"054adb7886447efe6f57e0368f06cf52b0a3370760d161cef126b91be7f89c421b62a6ec1da3c311d75ed50e0ab5fff3fd338acc3aa8a4e77ee26369acb81ba900fa83f5300cf9bb6c53ad1dc8a178b815db4235a9a9da0c06de4e615ea1277ce559e9c108de58c14a81aa77f5a6f8d1335494498848c8b95940740be7bf7c3705":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"0ca2ad77797ece86de5bf768750ddb5ed6a3116ad99bbd17edf7f782f0db1cd05b0f677468c5ea420dc116b10e80d110de2b0461ea14a38be68620392e7e893cb4ea9393fb886c2

0ff790642305bf302003892e54df9f667509dc53920df583f50a3dd61abb6fab75d600377e383e6aca6710eeea27156e0
6752c94ce25ae99fcbf8592dbe2d7e27453cb44de07100ebb1a2a19811a478adbeab270f94e8fe369d90b3ca612f9f":"2
2d71d54363a4217aa55113f059b3384e3e57e44":"049d0185845a264d28feb1e69edaec090609e8e46d93abb38371ce5
1f4aa65a599bdaaa81d24fba66a08a116cb644f3f1e653d95c89db8bbd5daac2709c8984000178410a7c6aa8667ddc38c
741f710ec8665aa9052be929d4e3b16782c1662114c5414bb0353455c392fc28f3db59054b5f365c49e1d156f876ee10
cb4fd70598":0

RSASSA-PSS
Signature Example 4_3
pkcs1_rsassa_pss_sign:1027:16:"029232336d2838945dba9dd7723f4e624a05f7375b927a87abe6a893a1658fd49f47f
6c7b0fa596c65fa68a23f0ab432962d18d4343bd6fd671a5ea8d148413995":16:"020ef5efe7c5394aed2272f7e81a74f4
c02d145894cb1b3cab23a9a0710a2afc7e3329acbb743d01f680c4d02afb4c8fde7e20930811bb2b995788b5e872c20bb
1":16:"054adb7886447efe6f57e0368f06cf52b0a3370760d161cef126b91be7f89c421b62a6ec1da3c311d75ed50e0ab
5fff3fd338acc3aa8a4e77ee26369acb81ba900fa83f5300cf9bb6c53ad1dc8a178b815db4235a9a9da0c06de4e615ea12
77ce559e9c108de58c14a81aa77f5a6f8d1335494498848c8b95940740be7bf7c3705":16:"010001":MBEDTLS_MD_
SHA1:MBEDTLS_MD_SHA1:"288062afc08fcdb7c5f8650b29837300461dd5676c17a20a3c8fb5148949e3f73d66b
3ae82c7240e27c5b3ec4328ee7d6ddf6a6a0c9b5b15bcda196a9d0c76b119d534d85abd123962d583b76ce9d180bce1c
a":"4af870fbc6516012ca916c70ba862ac7e8243617":"03fbc410a2ced59500fb99f9e2af2781ada74e13145624602782
e2994813eefca0519ecd253b855fb626a90d771eae028b0c47a199cbd9f8e3269734af4163599090713a3fa910fa09606
52721432b971036a7181a2bc0cab43b0b598bc6217461d7db305ff7e954c5b5bb231c39e791af6bcfa76b147b081321f
72641482a2aad":0

RSASSA-PSS
Signature Example 4_3 (verify)
pkcs1_rsassa_pss_verify:1027:16:"054adb7886447efe6f57e0368f06cf52b0a3370760d161cef126b91be7f89c421b62
a6ec1da3c311d75ed50e0ab5fff3fd338acc3aa8a4e77ee26369acb81ba900fa83f5300cf9bb6c53ad1dc8a178b815db42
35a9a9da0c06de4e615ea1277ce559e9c108de58c14a81aa77f5a6f8d1335494498848c8b95940740be7bf7c3705":16:"
010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"288062afc08fcdb7c5f8650b29837300461dd5676c17a2
0a3c8fb5148949e3f73d66b3ae82c7240e27c5b3ec4328ee7d6ddf6a6a0c9b5b15bcda196a9d0c76b119d534d85abd12
3962d583b76ce9d180bce1ca":"4af870fbc6516012ca916c70ba862ac7e8243617":"03fbc410a2ced59500fb99f9e2af2
781ada74e13145624602782e2994813eefca0519ecd253b855fb626a90d771eae028b0c47a199cbd9f8e3269734af4163
599090713a3fa910fa0960652721432b971036a7181a2bc0cab43b0b598bc6217461d7db305ff7e954c5b5bb231c39e7
91af6bcfa76b147b081321f72641482a2aad":0

RSASSA-PSS
Signature Example 4_4
pkcs1_rsassa_pss_sign:1027:16:"029232336d2838945dba9dd7723f4e624a05f7375b927a87abe6a893a1658fd49f47f
6c7b0fa596c65fa68a23f0ab432962d18d4343bd6fd671a5ea8d148413995":16:"020ef5efe7c5394aed2272f7e81a74f4
c02d145894cb1b3cab23a9a0710a2afc7e3329acbb743d01f680c4d02afb4c8fde7e20930811bb2b995788b5e872c20bb
1":16:"054adb7886447efe6f57e0368f06cf52b0a3370760d161cef126b91be7f89c421b62a6ec1da3c311d75ed50e0ab
5fff3fd338acc3aa8a4e77ee26369acb81ba900fa83f5300cf9bb6c53ad1dc8a178b815db4235a9a9da0c06de4e615ea12
77ce559e9c108de58c14a81aa77f5a6f8d1335494498848c8b95940740be7bf7c3705":16:"010001":MBEDTLS_MD_
SHA1:MBEDTLS_MD_SHA1:"6f4f9ab9501199cef55c6cf408fe7b36c557c49d420a4763d2463c8ad44b3cfc5be274
2c0e7d9b0f6608f08c7f47b693ee":"40d2e180fae1eac439c190b56c2c0e14ddf9a226":"0486644bc66bf75d28335a617
9b10851f43f09bded9fac1af33252bb9953ba4298cd6466b27539a70adaa3f89b3db3c74ab635d122f4ee7ce557a61e59
b82ffb786630e5f9db53c77d9a0c12fab5958d4c2ce7daa807cd89ba2cc7fcd02ff470ca67b229fcce814c852c73cc93bea
35be68459ce478e9d4655d121c8472f371d4f":0

RSASSA-PSS
Signature Example 4_4 (verify)
pkcs1_rsassa_pss_verify:1027:16:"054adb7886447efe6f57e0368f06cf52b0a3370760d161cef126b91be7f89c421b62
a6ec1da3c311d75ed50e0ab5fff3fd338acc3aa8a4e77ee26369acb81ba900fa83f5300cf9bb6c53ad1dc8a178b815db42
35a9a9da0c06de4e615ea1277ce559e9c108de58c14a81aa77f5a6f8d1335494498848c8b95940740be7bf7c3705":16:"
010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"6f4f9ab9501199cef55c6cf408fe7b36c557c49d420a476
3d2463c8ad44b3cfc5be2742c0e7d9b0f6608f08c7f47b693ee":"40d2e180fae1eac439c190b56c2c0e14ddf9a226":"04
86644bc66bf75d28335a6179b10851f43f09bded9fac1af33252bb9953ba4298cd6466b27539a70adaa3f89b3db3c74ab
635d122f4ee7ce557a61e59b82ffb786630e5f9db53c77d9a0c12fab5958d4c2ce7daa807cd89ba2cc7fcd02ff470ca67b
229fcce814c852c73cc93bea35be68459ce478e9d4655d121c8472f371d4f":0

RSASSA-PSS Signature Example 4_5
pkcs1_rsassa_pss_sign:1027:16:"029232336d2838945dba9dd7723f4e624a05f7375b927a87abe6a893a1658fd49f47f
6c7b0fa596c65fa68a23f0ab432962d18d4343bd6fd671a5ea8d148413995":16:"020ef5efe7c5394aed2272f7e81a74f4
c02d145894cb1b3cab23a9a0710a2afc7e3329acbb743d01f680c4d02afb4c8fde7e20930811bb2b995788b5e872c20bb
1":16:"054adb7886447efe6f57e0368f06cf52b0a3370760d161cef126b91be7f89c421b62a6ec1da3c311d75ed50e0ab
5fff3fd338acc3aa8a4e77ee26369acb81ba900fa83f5300cf9bb6c53ad1dc8a178b815db4235a9a9da0c06de4e615ea12
77ce559e9c108de58c14a81aa77f5a6f8d1335494498848c8b95940740be7bf7c3705":16:"010001":MBEDTLS_MD_
SHA1:MBEDTLS_MD_SHA1:"e17d20385d501955823c3f666254c1d3dd36ad5168b8f18d286fdcf67a7dad9409708
5fab7ed86fe2142a28771717997ef1a7a08884efc39356d76077aaf82459a7fad45848875f2819b098937fe923bcc9dc44
2d72d754d812025090c9bc03db3080c138dd63b355d0b4b85d6688ac19f4de15084a0ba4e373b93ef4a555096691915
dc23c00e954cdeb20a47cd55d16c3d8681d46ed7f2ed5ea42795be17baed25f0f4d113b3636addd585f16a8b5aec0c8fa
9c5f03cbf3b9b73":"2497dc2b4615dfae5a663d49ffd56bf7efc11304":"022a80045353904cb30cbb542d7d4990421a6e
ec16a8029a8422adfd22d6aff8c4cc0294af110a0c067ec86a7d364134459bb1ae8ff836d5a8a2579840996b320b19f13a
13fad378d931a65625dae2739f0c53670b35d9d3cbac08e733e4ec2b83af4b9196d63e7c4ff1ddeae2a122791a125bfea8
deb0de8ccf1f4ffaf6e6fb0a":0

RSASSA-PSS
Signature Example 4_5 (verify)
pkcs1_rsassa_pss_verify:1027:16:"054adb7886447efe6f57e0368f06cf52b0a3370760d161cef126b91be7f89c421b62
a6ec1da3c311d75ed50e0ab5fff3fd338acc3aa8a4e77ee26369acb81ba900fa83f5300cf9bb6c53ad1dc8a178b815db42
35a9a9da0c06de4e615ea1277ce559e9c108de58c14a81aa77f5a6f8d1335494498848c8b95940740be7bf7c3705":16:"
010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"e17d20385d501955823c3f666254c1d3dd36ad5168b8f1
8d286fdcf67a7dad94097085fab7ed86fe2142a28771717997ef1a7a08884efc39356d76077aaf82459a7fad45848875f2
819b098937fe923bcc9dc442d72d754d812025090c9bc03db3080c138dd63b355d0b4b85d6688ac19f4de15084a0ba4
e373b93ef4a555096691915dc23c00e954cdeb20a47cd55d16c3d8681d46ed7f2ed5ea42795be17baed25f0f4d113b36
36addd585f16a8b5aec0c8fa9c5f03cbf3b9b73":"2497dc2b4615dfae5a663d49ffd56bf7efc11304":"022a80045353904
cb30cbb542d7d4990421a6eec16a8029a8422adfd22d6aff8c4cc0294af110a0c067ec86a7d364134459bb1ae8ff836d5a
8a2579840996b320b19f13a13fad378d931a65625dae2739f0c53670b35d9d3cbac08e733e4ec2b83af4b9196d63e7c4f
f1ddeae2a122791a125bfea8deb0de8ccf1f4ffaf6e6fb0a":0

RSASSA-PSS
Signature Example 4_6
pkcs1_rsassa_pss_sign:1027:16:"029232336d2838945dba9dd7723f4e624a05f7375b927a87abe6a893a1658fd49f47f
6c7b0fa596c65fa68a23f0ab432962d18d4343bd6fd671a5ea8d148413995":16:"020ef5efe7c5394aed2272f7e81a74f4
c02d145894cb1b3cab23a9a0710a2afc7e3329acbb743d01f680c4d02afb4c8fde7e20930811bb2b995788b5e872c20bb
1":16:"054adb7886447efe6f57e0368f06cf52b0a3370760d161cef126b91be7f89c421b62a6ec1da3c311d75ed50e0ab
5fff3fd338acc3aa8a4e77ee26369acb81ba900fa83f5300cf9bb6c53ad1dc8a178b815db4235a9a9da0c06de4e615ea12

77ce559e9c108de58c14a81aa77f5a6f8d1335494498848c8b95940740be7bf7c3705":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"afbc19d479249018fdf4e09f618726440495de11ddeee38872d775fcea74a23896b5343c9c38d46af0dba224d047580cc60a65e9391cf9b59b36a860598d4e8216722f993b91cfae87bc255af89a6a199bca4a391eadbc3a24903c0bd667368f6be78e3feabfb4ffd463122763740ffbbefeab9a25564bc5d1c24c93e422f75073e2ad72bf45b10df00b52a147128e73fee33fa3f0577d77f80fbc2df1bed313290c12777f50":"a334db6faebf11081a04f87c2d621cdec7930b9b":"00938dcb6d583046065f69c78da7a1f1757066a7fa75125a9d2929f0b79a60b627b082f11f5b196f28eb9daa6f21c05e5140f6aef1737d2023075c05ecf04a028c686a2ab3e7d5a0664f295ce12995e890908b6ad21f0839eb65b70393a7b5afd9871de0caa0cedec5b819626756209d13ab1e7bb9546a26ff37e9a51af9fd562e":0

RSASSA-PSS

Signature Example 4_6 (verify)

pkcs1_rsassa_pss_verify:1027:16:"054adb7886447efe6f57e0368f06cf52b0a3370760d161cef126b91be7f89c421b62a6ec1da3c311d75ed50e0ab5fff3fd338acc3aa8a4e77ee26369acb81ba900fa83f5300cf9bb6c53ad1dc8a178b815db4235a9a9da0c06de4e615ea1277ce559e9c108de58c14a81aa77f5a6f8d1335494498848c8b95940740be7bf7c3705":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"afbc19d479249018fdf4e09f618726440495de11ddeee38872d775fcea74a23896b5343c9c38d46af0dba224d047580cc60a65e9391cf9b59b36a860598d4e8216722f993b91cfae87bc255af89a6a199bca4a391eadbc3a24903c0bd667368f6be78e3feabfb4ffd463122763740ffbbefeab9a25564bc5d1c24c93e422f75073e2ad72bf45b10df00b52a147128e73fee33fa3f0577d77f80fbc2df1bed313290c12777f50":"a334db6faebf11081a04f87c2d621cdec7930b9b":"00938dcb6d583046065f69c78da7a1f1757066a7fa75125a9d2929f0b79a60b627b082f11f5b196f28eb9daa6f21c05e5140f6aef1737d2023075c05ecf04a028c686a2ab3e7d5a0664f295ce12995e890908b6ad21f0839eb65b70393a7b5afd9871de0caa0cedec5b819626756209d13ab1e7bb9546a26ff37e9a51af9fd562e":0

RSASSA-PSS

Signature Example 5_1

pkcs1_rsassa_pss_sign:1028:16:"03f2f331f4142d4f24b43aa10279a89652d4e7537221a1a7b2a25deb551e5de9ac497411c227a94e45f91c2d1c13cc046cf4ce14e32d058734210d44a87ee1b73f":16:"034f090d73b55803030cf0361a5d8081bfb79f851523feac0a2124d08d4013ff08487771a870d0479dc0686c62f7718dfecf024b17c9267678059171339cc00839":16:"0d10f661f29940f5ed39aa260966deb47843679d2b6fb25b3de370f3ac7c19916391fd25fb527ebfa6a4b4df45a1759d996c4bb4ebd18828c44fc52d0191871740525f47a4b0cc8da325ed8aa676b0d0f626e0a77f07692170acac8082f42faa7dc7cd123e730e31a87985204cabcbe6670d43a2dd2b2ddef5e05392fc213bc507":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"30c7d557458b436decfdc14d06cb7b96b06718c48d7de57482a868ae7f065870a6216506d11b779323dfdf046cf5775129134b4d5689e4d9c0ce1e12d7d4b06cb5fc5820decfa41baf59bf257b32f025b7679b445b9499c92555145885992f1b76f84891ee4d3be0f5150fd5901e3a4c8ed43fd36b61d022e65ad5008dbf33293c22bfbfd07321f0f1d5fa9fdf0014c2fcb0358aad0e354b0d29":"081b233b43567750bd6e78f396a88b9f6a445151":"0ba373f76e0921b70a8fbfe622f0bf77b28a3db98e361051c3d7cb92ad0452915a4de9c01722f6823eeb6adf7e0ca8290f5de3e549890ac2a3c5950ab217ba58590894952de96f8df111b2575215da6c161590c745be612476ee578ed384ab33e3ece97481a252f5c79a98b5532ae00cdd62f2ecc0cd1baefe80d80b962193ec1d":0

RSASSA-PSS

Signature Example 5_1 (verify)

pkcs1_rsassa_pss_verify:1028:16:"0d10f661f29940f5ed39aa260966deb47843679d2b6fb25b3de370f3ac7c19916391fd25fb527ebfa6a4b4df45a1759d996c4bb4ebd18828c44fc52d0191871740525f47a4b0cc8da325ed8aa676b0d0f626e0a77f07692170acac8082f42faa7dc7cd123e730e31a87985204cabcbe6670d43a2dd2b2ddef5e05392fc213bc507":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"30c7d557458b436decfdc14d06cb7b96b06718c48d7de57482a868ae7f065870a6216506d11b779323dfdf046cf5775129134b4d5689e4d9c0ce1e12d7d4b06cb5fc5820decfa41baf59bf257b32f025b7679b445b9499c92555145885992f1b76f84891ee4d3be0f5150fd5901e3a4c8ed43fd36b61d022e65ad5008dbf33293c22bfbfd07321f0f1d5fa9fdf0014c2fcb0358aad0e354b0d29":"081b233b43567750bd6e78f39

6a88b9f6a445151":"0ba373f76e0921b70a8fbfe622f0bf77b28a3db98e361051c3d7cb92ad0452915a4de9c01722f6823eeb6adf7e0ca8290f5de3e549890ac2a3c5950ab217ba58590894952de96f8df111b2575215da6c161590c745be612476ee578ed384ab33e3ece97481a252f5c79a98b5532ae00cdd62f2ecc0cd1baefe80d80b962193ec1d":0

RSASSA-PSS

Signature Example 5_2

pkcs1_rsassa_pss_sign:1028:16:"03f2f331f4142d4f24b43aa10279a89652d4e7537221a1a7b2a25deb551e5de9ac497411c227a94e45f91c2d1c13cc046cf4ce14e32d058734210d44a87ee1b73f":16:"034f090d73b55803030cf0361a5d8081bfb79f851523feac0a2124d08d4013ff08487771a870d0479dc0686c62f7718dfecf024b17c9267678059171339cc00839":16:"0d10f661f29940f5ed39aa260966deb47843679d2b6fb25b3de370f3ac7c19916391fd25fb527ebfa6a4b4df45a1759d996c4bb4ebd18828c44fc52d0191871740525f47a4b0cc8da325ed8aa676b0d0f626e0a77f07692170acac8082f42faa7dc7cd123e730e31a87985204cabcbe6670d43a2dd2b2ddef5e05392fc213bc507":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"e7b32e1556ea1b2795046ac69739d22ac8966bf11c116f614b166740e96b90653e5750945fcf772186c03790a07fda323e1a61916b06ee2157db3dff80d67d5e39a53ae268c8f09ed99a732005b0bc6a04af4e08d57a00e7201b3060efaadb73113bfc087fd837093aa25235b8c149f56215f031c24ad5bde7f29960df7d524070f7449c6f785084be1a0f733047f336f9154738674547db02a9f44dfc6e60301081e1ce99847f3b5b601ff06b4d5776a9740b9aa0d34058fd3b906e4f7859dfb07d7173e5e6f6350adac21f27b2307469":"bd0ce19549d0700120cbe51077dbbbb00a8d8b09":"08180de825e4b8b014a32da8ba761555921204f2f90d5f24b712908ff84f3e220ad17997c0dd6e706630ba3e84add4d5e7ab004e58074b549709565d43ad9e97b5a7a1a29e85b9f90f4aafcdf58321de8c5974ef9abf2d526f33c0f2f82e95d158ea6b81f1736db8d1af3d6ac6a83b32d18bae0ff1b2fe27de4c76ed8c7980a34e":0

RSASSA-PSS

Signature Example 5_2 (verify)

pkcs1_rsassa_pss_verify:1028:16:"0d10f661f29940f5ed39aa260966deb47843679d2b6fb25b3de370f3ac7c19916391fd25fb527ebfa6a4b4df45a1759d996c4bb4ebd18828c44fc52d0191871740525f47a4b0cc8da325ed8aa676b0d0f626e0a77f07692170acac8082f42faa7dc7cd123e730e31a87985204cabcbe6670d43a2dd2b2ddef5e05392fc213bc507":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"e7b32e1556ea1b2795046ac69739d22ac8966bf11c116f614b166740e96b90653e5750945fcf772186c03790a07fda323e1a61916b06ee2157db3dff80d67d5e39a53ae268c8f09ed99a732005b0bc6a04af4e08d57a00e7201b3060efaadb73113bfc087fd837093aa25235b8c149f56215f031c24ad5bde7f29960df7d524070f7449c6f785084be1a0f733047f336f9154738674547db02a9f44dfc6e60301081e1ce99847f3b5b601ff06b4d5776a9740b9aa0d34058fd3b906e4f7859dfb07d7173e5e6f6350adac21f27b2307469":"bd0ce19549d0700120cbe51077dbbbb00a8d8b09":"08180de825e4b8b014a32da8ba761555921204f2f90d5f24b712908ff84f3e220ad17997c0dd6e706630ba3e84add4d5e7ab004e58074b549709565d43ad9e97b5a7a1a29e85b9f90f4aafcdf58321de8c5974ef9abf2d526f33c0f2f82e95d158ea6b81f1736db8d1af3d6ac6a83b32d18bae0ff1b2fe27de4c76ed8c7980a34e":0

RSASSA-PSS

Signature Example 5_3

pkcs1_rsassa_pss_sign:1028:16:"03f2f331f4142d4f24b43aa10279a89652d4e7537221a1a7b2a25deb551e5de9ac497411c227a94e45f91c2d1c13cc046cf4ce14e32d058734210d44a87ee1b73f":16:"034f090d73b55803030cf0361a5d8081bfb79f851523feac0a2124d08d4013ff08487771a870d0479dc0686c62f7718dfecf024b17c9267678059171339cc00839":16:"0d10f661f29940f5ed39aa260966deb47843679d2b6fb25b3de370f3ac7c19916391fd25fb527ebfa6a4b4df45a1759d996c4bb4ebd18828c44fc52d0191871740525f47a4b0cc8da325ed8aa676b0d0f626e0a77f07692170acac8082f42faa7dc7cd123e730e31a87985204cabcbe6670d43a2dd2b2ddef5e05392fc213bc507":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"8d8396e36507fe1ef6a19017548e0c716674c2fec233adb2f775665ec41f2bd0ba396b061a9daa7e866f7c23fd3531954300a342f924535ea1498c48f6c879932865fc02000c528723b7ad0335745b51209a0afed932af8f0887c219004d2abd894ea92559ee3198af3a734fe9b9638c263a728ad95a5ae8ce3eb15839f3aa7852bb390706e7760e43a71291a2e3f827237deda851874c517665f545f27238df86557f375d09ccd8bd15d8ccf61f5d78ca5c7f5cde782e6bf5d0057056d4bad98b3d2f9575e824ab7a33ff57b0ac100ab0d6ead7aa0b50f6e4d3e5ec0b966b":"815779a91b

3a8bd049bf2aeb920142772222c9ca":"05e0fdbdf6f756ef733185ccfa8ced2eb6d029d9d56e35561b5db8e70257ee6fd019d2f0bbf669fe9b9821e78df6d41e31608d58280f318ee34f559941c8df13287574bac000b7e58dc4f414ba49fb127f9d0f8936638c76e85356c994f79750f7fa3cf4fd482df75e3fb9978cd061f7abb17572e6e63e0bde12cbdcf18c68b979":0

RSASSA-PSS

Signature Example 5_3 (verify)

pkcs1_rsassa_pss_verify:1028:16:"0d10f661f29940f5ed39aa260966deb47843679d2b6fb25b3de370f3ac7c19916391fd25fb527ebfa6a4b4df45a1759d996c4bb4ebd18828c44fc52d0191871740525f47a4b0cc8da325ed8aa676b0d0f626e0a77f07692170acac8082f42faa7dc7cd123e730e31a87985204cabcbe6670d43a2dd2b2ddef5e05392fc213bc507":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"8d8396e36507fe1ef6a19017548e0c716674c2fec233adb2f775665ec41f2bd0ba396b061a9daa7e866f7c23fd3531954300a342f924535ea1498c48f6c879932865fc02000c528723b7ad0335745b51209a0afed932af8f0887c219004d2abd894ea92559ee3198af3a734fe9b9638c263a728ad95a5ae8ce3eb15839f3aa7852bb390706e7760e43a71291a2e3f827237deda851874c517665f545f27238df86557f375d09ccd8bd15d8ccf61f5d78ca5c7f5cde782e6bf5d0057056d4bad98b3d2f9575e824ab7a33ff57b0ac100ab0d6ead7aa0b50f6e4d3e5ec0b966b":"815779a91b3a8bd049bf2aeb920142772222c9ca":"05e0fdbdf6f756ef733185ccfa8ced2eb6d029d9d56e35561b5db8e70257ee6fd019d2f0bbf669fe9b9821e78df6d41e31608d58280f318ee34f559941c8df13287574bac000b7e58dc4f414ba49fb127f9d0f8936638c76e85356c994f79750f7fa3cf4fd482df75e3fb9978cd061f7abb17572e6e63e0bde12cbdcf18c68b979":0

RSASSA-PSS

Signature Example 5_4

pkcs1_rsassa_pss_sign:1028:16:"03f2f331f4142d4f24b43aa10279a89652d4e7537221a1a7b2a25deb551e5de9ac497411c227a94e45f91c2d1c13cc046cf4ce14e32d058734210d44a87ee1b73f":16:"034f090d73b55803030cf0361a5d8081bfb79f851523feac0a2124d08d4013ff08487771a870d0479dc0686c62f7718dfecf024b17c9267678059171339cc00839":16:"0d10f661f29940f5ed39aa260966deb47843679d2b6fb25b3de370f3ac7c19916391fd25fb527ebfa6a4b4df45a1759d996c4bb4ebd18828c44fc52d0191871740525f47a4b0cc8da325ed8aa676b0d0f626e0a77f07692170acac8082f42faa7dc7cd123e730e31a87985204cabcbe6670d43a2dd2b2ddef5e05392fc213bc507":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"328c659e0a6437433cceb73c14":"9aec4a7480d5bbc42920d7ca235db674989c9aac":"0bc989853bc2ea86873271ce183a923ab65e8a53100e6df5d87a24c4194eb797813ee2a187c097dd872d591da60c568605dd7e742d5af4e33b11678ccb63903204a3d080b0902c89aba8868f009c0f1c0cb85810bbdd29121abb8471ff2d39e49fd92d56c655c8e037ad18fafbdc92c95863f7f61ea9efa28fea401369d19daea1":0

RSASSA-PSS

Signature Example 5_4 (verify)

pkcs1_rsassa_pss_verify:1028:16:"0d10f661f29940f5ed39aa260966deb47843679d2b6fb25b3de370f3ac7c19916391fd25fb527ebfa6a4b4df45a1759d996c4bb4ebd18828c44fc52d0191871740525f47a4b0cc8da325ed8aa676b0d0f626e0a77f07692170acac8082f42faa7dc7cd123e730e31a87985204cabcbe6670d43a2dd2b2ddef5e05392fc213bc507":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"328c659e0a6437433cceb73c14":"9aec4a7480d5bbc42920d7ca235db674989c9aac":"0bc989853bc2ea86873271ce183a923ab65e8a53100e6df5d87a24c4194eb797813ee2a187c097dd872d591da60c568605dd7e742d5af4e33b11678ccb63903204a3d080b0902c89aba8868f009c0f1c0cb85810bbdd29121abb8471ff2d39e49fd92d56c655c8e037ad18fafbdc92c95863f7f61ea9efa28fea401369d19daea1":0

RSASSA-PSS

Signature Example 5_5

pkcs1_rsassa_pss_sign:1028:16:"03f2f331f4142d4f24b43aa10279a89652d4e7537221a1a7b2a25deb551e5de9ac497411c227a94e45f91c2d1c13cc046cf4ce14e32d058734210d44a87ee1b73f":16:"034f090d73b55803030cf0361a5d8081bfb79f851523feac0a2124d08d4013ff08487771a870d0479dc0686c62f7718dfecf024b17c9267678059171339cc00839":16:"0d10f661f29940f5ed39aa260966deb47843679d2b6fb25b3de370f3ac7c19916391fd25fb527ebfa6a4b4df45a

1759d996c4bb4ebd18828c44fc52d0191871740525f47a4b0cc8da325ed8aa676b0d0f626e0a77f07692170acac8082f4
2faa7dc7cd123e730e31a87985204cabcbe6670d43a2dd2b2ddef5e05392fc213bc507":16:"010001":MBEDTLS_MD
_SHA1:MBEDTLS_MD_SHA1:"f37b962379a47d415a376eec8973150bcb34edd5ab654041b61430560c2144582ba
133c867d852d6b8e23321901302ecb45b09ec88b1527178fa043263f3067d9ffe973032a99f4cb08ad2c7e0a2456cdd5
7a7df56fe6053527a5aeb67d7e552063c1ca97b1beffa7b39e997caf27878ea0f62cbebc8c21df4c889a202851e9490884
90c249b6e9acf1d8063f5be2343989bf95c4da01a2be78b4ab6b378015bc37957f76948b5e58e440c28453d40d7cfd57e
7d690600474ab5e75973b1ea0c5f1e45d14190afe2f4eb6d3bdf71f1d2f8bb156a1c295d04aaeb9d689dce79ed62bc443
e":"e20c1e9878512c39970f58375e1549a68b64f31d":"0aefa943b698b9609edf898ad22744ac28dc239497cea369cbb
d84f65c95c0ad776b594740164b59a739c6ff7c2f07c7c077a86d95238fe51e1fcf33574a4ae0684b42a3f6bf677d91820
ca89874467b2c23add77969c80717430d0efc1d3695892ce855cb7f7011630f4df26def8ddf36fc23905f57fa6243a485c
770d5681fcd":0

RSASSA-PSS
Signature
Example 5_5 (verify)
pkcs1_rsassa_pss_verify:1028:16:"0d10f661f29940f5ed39aa260966deb47843679d2b6fb25b3de370f3ac7c1991639
1fd25fb527ebfa6a4b4df45a1759d996c4bb4ebd18828c44fc52d0191871740525f47a4b0cc8da325ed8aa676b0d0f626
e0a77f07692170acac8082f42faa7dc7cd123e730e31a87985204cabcbe6670d43a2dd2b2ddef5e05392fc213bc507":16
:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"f37b962379a47d415a376eec8973150bcb34edd5ab654
041b61430560c2144582ba133c867d852d6b8e23321901302ecb45b09ec88b1527178fa043263f3067d9ffe973032a99
f4cb08ad2c7e0a2456cdd57a7df56fe6053527a5aeb67d7e552063c1ca97b1beffa7b39e997caf27878ea0f62cbebc8c21
df4c889a202851e949088490c249b6e9acf1d8063f5be2343989bf95c4da01a2be78b4ab6b378015bc37957f76948b5e
58e440c28453d40d7cfd57e7d690600474ab5e75973b1ea0c5f1e45d14190afe2f4eb6d3bdf71f1d2f8bb156a1c295d04
aaeb9d689dce79ed62bc443e":"e20c1e9878512c39970f58375e1549a68b64f31d":"0aefa943b698b9609edf898ad227
44ac28dc239497cea369cbbd84f65c95c0ad776b594740164b59a739c6ff7c2f07c7c077a86d95238fe51e1fcf33574a4a
e0684b42a3f6bf677d91820ca89874467b2c23add77969c80717430d0efc1d3695892ce855cb7f7011630f4df26def8dd
f36fc23905f57fa6243a485c770d5681fcd":0

RSASSA-PSS
Signature Example 5_6
pkcs1_rsassa_pss_sign:1028:16:"03f2f331f4142d4f24b43aa10279a89652d4e7537221a1a7b2a25deb551e5de9ac497
411c227a94e45f91c2d1c13cc046cf4ce14e32d058734210d44a87ee1b73f":16:"034f090d73b55803030cf0361a5d808
1bfb79f851523feac0a2124d08d4013ff08487771a870d0479dc0686c62f7718dfecf024b17c9267678059171339cc008
39":16:"0d10f661f29940f5ed39aa260966deb47843679d2b6fb25b3de370f3ac7c19916391fd25fb527ebfa6a4b4df45a
1759d996c4bb4ebd18828c44fc52d0191871740525f47a4b0cc8da325ed8aa676b0d0f626e0a77f07692170acac8082f4
2faa7dc7cd123e730e31a87985204cabcbe6670d43a2dd2b2ddef5e05392fc213bc507":16:"010001":MBEDTLS_MD
_SHA1:MBEDTLS_MD_SHA1:"c6103c330c1ef718c141e47b8fa859be4d5b96259e7d142070ecd485839dba5a8369
c17c1114035e532d195c74f44a0476a2d3e8a4da210016caced0e367cb867710a4b5aa2df2b8e5daf5fdc647807d4d5eb
b6c56b9763ccdae4dea3308eb0ac2a89501cb209d2639fa5bf87ce790747d3cb2d295e84564f2f637824f0c13028129b0
aa4a422d162282":"23291e4a3307e8bbb776623ab34e4a5f4cc8a8db":"02802dccfa8dfaf5279bf0b4a29ba1b157611fa
eaaf419b8919d15941900c1339e7e92e6fae562c53e6cc8e84104b110bce03ad18525e3c49a0eadad5d3f28f244a8ed89
edbafbb686277cfa8ae909714d6b28f4bf8e293aa04c41efe7c0a81266d5c061e2575be032aa464674ff71626219bd74cc
45f0e7ed4e3ff96eee758e8f":0

RSASSA-PSS
Signature Example 5_6 (verify)
pkcs1_rsassa_pss_verify:1028:16:"0d10f661f29940f5ed39aa260966deb47843679d2b6fb25b3de370f3ac7c1991639
1fd25fb527ebfa6a4b4df45a1759d996c4bb4ebd18828c44fc52d0191871740525f47a4b0cc8da325ed8aa676b0d0f626

e0a77f07692170acac8082f42faa7dc7cd123e730e31a87985204cabcbe6670d43a2dd2b2ddef5e05392fc213bc507":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"c6103c330c1ef718c141e47b8fa859be4d5b96259e7d142070ecd485839dba5a8369c17c1114035e532d195c74f44a0476a2d3e8a4da210016caced0e367cb867710a4b5aa2df2b8e5daf5fdc647807d4d5ebb6c56b9763ccdae4dea3308eb0ac2a89501cb209d2639fa5bf87ce790747d3cb2d295e84564f2f637824f0c13028129b0aa4a422d162282":"23291e4a3307e8bbb776623ab34e4a5f4cc8a8db":"02802dccfa8dfaf5279bf0b4a29ba1b157611faeaaf419b8919d15941900c1339e7e92e6fae562c53e6cc8e84104b110bce03ad18525e3c49a0eadad5d3f28f244a8ed89edbafbb686277cfa8ae909714d6b28f4bf8e293aa04c41efe7c0a81266d5c061e2575be032aa464674ff71626219bd74cc45f0e7ed4e3ff96eee758e8f":0

RSASSA-PSS

Signature Example 6_1

pkcs1_rsassa_pss_sign:1029:16:"04f0548c9626ab1ebf1244934741d99a06220efa2a5856aa0e75730b2ec96adc86be894fa2803b53a5e85d276acbd29ab823f80a7391bb54a5051672fb04eeb543":16:"0483e0ae47915587743ff345362b555d3962d98bb6f15f848b4c92b1771ca8ed107d8d3ee65ec44517dd0faa481a387e902f7a2e747c269e7ea44480bc538b8e5b":16:"164ca31cff609f3a0e7101b039f2e4fe6dd37519ab98598d179e174996598071f47d3a04559158d7be373cf1aa53f0aa6ef09039e5678c2a4c63900514c8c4f8aaed5de12a5f10b09c311af8c0ffb5b7a297f2efc63b8d6b0510931f0b98e48bf5fc6ec4e7b8db1ffaeb08c38e02adb8f03a48229c99e969431f61cb8c4dc698d1":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"0a20b774addc2fa51245ed7cb9da609e50cac6636a52543f97458eed7340f8d53ffc64918f949078ee03ef60d42b5fec246050bd5505cd8cb597bad3c4e713b0ef30644e76adabb0de01a1561efb255158c74fc801e6e919e581b46f0f0ddd08e4f34c7810b5ed8318f91d7c8c":"5b4ea2ef629cc22f3b538e016904b47b1e40bfd5":"04c0cfacec04e5badbece159a5a1103f69b3f32ba593cb4cc4b1b7ab455916a96a27cd2678ea0f46ba37f7fc9c86325f29733b389f1d97f43e7201c0f348fc45fe42892335362eee018b5b161f2f9393031225c713012a576bc88e23052489868d9010cbf033ecc568e8bc152bdc59d560e41291915d28565208e22aeec9ef85d1":0

RSASSA-PSS

Signature Example 6_1 (verify)

pkcs1_rsassa_pss_verify:1029:16:"164ca31cff609f3a0e7101b039f2e4fe6dd37519ab98598d179e174996598071f47d3a04559158d7be373cf1aa53f0aa6ef09039e5678c2a4c63900514c8c4f8aaed5de12a5f10b09c311af8c0ffb5b7a297f2efc63b8d6b0510931f0b98e48bf5fc6ec4e7b8db1ffaeb08c38e02adb8f03a48229c99e969431f61cb8c4dc698d1":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"0a20b774addc2fa51245ed7cb9da609e50cac6636a52543f97458eed7340f8d53ffc64918f949078ee03ef60d42b5fec246050bd5505cd8cb597bad3c4e713b0ef30644e76adabb0de01a1561efb255158c74fc801e6e919e581b46f0f0ddd08e4f34c7810b5ed8318f91d7c8c":"5b4ea2ef629cc22f3b538e016904b47b1e40bfd5":"04c0cfacec04e5badbece159a5a1103f69b3f32ba593cb4cc4b1b7ab455916a96a27cd2678ea0f46ba37f7fc9c86325f29733b389f1d97f43e7201c0f348fc45fe42892335362eee018b5b161f2f9393031225c713012a576bc88e23052489868d9010cbf033ecc568e8bc152bdc59d560e41291915d28565208e22aeec9ef85d1":0

RSASSA-PSS

Signature Example 6_2

pkcs1_rsassa_pss_sign:1029:16:"04f0548c9626ab1ebf1244934741d99a06220efa2a5856aa0e75730b2ec96adc86be894fa2803b53a5e85d276acbd29ab823f80a7391bb54a5051672fb04eeb543":16:"0483e0ae47915587743ff345362b555d3962d98bb6f15f848b4c92b1771ca8ed107d8d3ee65ec44517dd0faa481a387e902f7a2e747c269e7ea44480bc538b8e5b":16:"164ca31cff609f3a0e7101b039f2e4fe6dd37519ab98598d179e174996598071f47d3a04559158d7be373cf1aa53f0aa6ef09039e5678c2a4c63900514c8c4f8aaed5de12a5f10b09c311af8c0ffb5b7a297f2efc63b8d6b0510931f0b98e48bf5fc6ec4e7b8db1ffaeb08c38e02adb8f03a48229c99e969431f61cb8c4dc698d1":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"2aaff6631f621ce615760a9ebce94bb333077ad86488c861d4b76d29c1f48746c611ae1e03ced4445d7cfa1fe5f62e1b3f08452bde3b6ef81973bafbb57f97bceef873985395b8260589aa88cb7db50ab469262e551bdcd9a56f275a0ac4fe484700c35f3dbf2b469ede864741b86fa59172a360ba95a02e139be50ddfb7cf0b42faeabbfbbaa86a4497699c4f2dfd5b08406af7e14144427c253ec0efa20eaf9a8be8cd49ce1f1bc4e93e619cf2aa8ed4fb39bc8590d

0f7b96488f7317ac9abf7bee4e3a0e715":"83146a9e782722c28b014f98b4267bda2ac9504f":"0a2314250cf52b6e4e90
8de5b35646bcaa24361da8160fb0f9257590ab3ace42b0dc3e77ad2db7c203a20bd952fbb56b1567046ecfaa933d7b10
00c3de9ff05b7d989ba46fd43bc4c2d0a3986b7ffa13471d37eb5b47d64707bd290cfd6a9f393ad08ec1e3bd71bb57926
15035cdaf2d8929aed3be098379377e777ce79aaa4773":0

RSASSA-PSS
Signature Example 6_2 (verify)
pkcs1_rsassa_pss_verify:1029:16:"164ca31cff609f3a0e7101b039f2e4fe6dd37519ab98598d179e174996598071f47d
3a04559158d7be373cf1aa53f0aa6ef09039e5678c2a4c63900514c8c4f8aaed5de12a5f10b09c311af8c0ffb5b7a297f2e
fc63b8d6b0510931f0b98e48bf5fc6ec4e7b8db1ffaeb08c38e02adb8f03a48229c99e969431f61cb8c4dc698d1":16:"01
0001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"2aaff6631f621ce615760a9ebce94bb333077ad86488c861d
4b76d29c1f48746c611ae1e03ced4445d7cfa1fe5f62e1b3f08452bde3b6ef81973bafbb57f97bceef873985395b826058
9aa88cb7db50ab469262e551bdcd9a56f275a0ac4fe484700c35f3dbf2b469ede864741b86fa59172a360ba95a02e139b
e50ddfb7cf0b42faeabbfbbaa86a4497699c4f2dfd5b08406af7e14144427c253ec0efa20eaf9a8be8cd49ce1f1bc4e93e6
19cf2aa8ed4fb39bc8590d0f7b96488f7317ac9abf7bee4e3a0e715":"83146a9e782722c28b014f98b4267bda2ac9504f"
:"0a2314250cf52b6e4e908de5b35646bcaa24361da8160fb0f9257590ab3ace42b0dc3e77ad2db7c203a20bd952fbb56
b1567046ecfaa933d7b1000c3de9ff05b7d989ba46fd43bc4c2d0a3986b7ffa13471d37eb5b47d64707bd290cfd6a9f39
3ad08ec1e3bd71bb5792615035cdaf2d8929aed3be098379377e777ce79aaa4773":0

RSASSA-PSS
Signature Example 6_3
pkcs1_rsassa_pss_sign:1029:16:"04f0548c9626ab1ebf1244934741d99a06220efa2a5856aa0e75730b2ec96adc86be8
94fa2803b53a5e85d276acbd29ab823f80a7391bb54a5051672fb04eeb543":16:"0483e0ae47915587743ff345362b55
5d3962d98bb6f15f848b4c92b1771ca8ed107d8d3ee65ec44517dd0faa481a387e902f7a2e747c269e7ea44480bc538b8
e5b":16:"164ca31cff609f3a0e7101b039f2e4fe6dd37519ab98598d179e174996598071f47d3a04559158d7be373cf1a
a53f0aa6ef09039e5678c2a4c63900514c8c4f8aaed5de12a5f10b09c311af8c0ffb5b7a297f2efc63b8d6b0510931f0b98
e48bf5fc6ec4e7b8db1ffaeb08c38e02adb8f03a48229c99e969431f61cb8c4dc698d1":16:"010001":MBEDTLS_MD_
SHA1:MBEDTLS_MD_SHA1:"0f6195d04a6e6fc7e2c9600dbf840c39ea8d4d624fd53507016b0e26858a5e0aecd7ad
a543ae5c0ab3a62599cba0a54e6bf446e262f989978f9ddf5e9a41":"a87b8aed07d7b8e2daf14ddca4ac68c4d0aabff8":"
086df6b500098c120f24ff8423f727d9c61a5c9007d3b6a31ce7cf8f3cbec1a26bb20e2bd4a046793299e03e37a21b401
94fb045f90b18bf20a47992ccd799cf9c059c299c0526854954aade8a6ad9d97ec91a1145383f42468b231f4d72f23706
d9853c3fa43ce8ace8bfe7484987a1ec6a16c8daf81f7c8bf42774707a9df456":0

RSASSA-PSS
Signature Example 6_3 (verify)
pkcs1_rsassa_pss_verify:1029:16:"164ca31cff609f3a0e7101b039f2e4fe6dd37519ab98598d179e174996598071f47d
3a04559158d7be373cf1aa53f0aa6ef09039e5678c2a4c63900514c8c4f8aaed5de12a5f10b09c311af8c0ffb5b7a297f2e
fc63b8d6b0510931f0b98e48bf5fc6ec4e7b8db1ffaeb08c38e02adb8f03a48229c99e969431f61cb8c4dc698d1":16:"01
0001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"0f6195d04a6e6fc7e2c9600dbf840c39ea8d4d624fd535070
16b0e26858a5e0aecd7ada543ae5c0ab3a62599cba0a54e6bf446e262f989978f9ddf5e9a41":"a87b8aed07d7b8e2daf1
4ddca4ac68c4d0aabff8":"086df6b500098c120f24ff8423f727d9c61a5c9007d3b6a31ce7cf8f3cbec1a26bb20e2bd4a0
46793299e03e37a21b40194fb045f90b18bf20a47992ccd799cf9c059c299c0526854954aade8a6ad9d97ec91a114538
3f42468b231f4d72f23706d9853c3fa43ce8ace8bfe7484987a1ec6a16c8daf81f7c8bf42774707a9df456":0

RSASSA-PSS
Signature Example 6_4
pkcs1_rsassa_pss_sign:1029:16:"04f0548c9626ab1ebf1244934741d99a06220efa2a5856aa0e75730b2ec96adc86be8
94fa2803b53a5e85d276acbd29ab823f80a7391bb54a5051672fb04eeb543":16:"0483e0ae47915587743ff345362b55

5d3962d98bb6f15f848b4c92b1771ca8ed107d8d3ee65ec44517dd0faa481a387e902f7a2e747c269e7ea44480bc538b8e5b":16:"164ca31cff609f3a0e7101b039f2e4fe6dd37519ab98598d179e174996598071f47d3a04559158d7be373cf1aa53f0aa6ef09039e5678c2a4c63900514c8c4f8aaed5de12a5f10b09c311af8c0ffb5b7a297f2efc63b8d6b0510931f0b98e48bf5fc6ec4e7b8db1ffaeb08c38e02adb8f03a48229c99e969431f61cb8c4dc698d1":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"337d25fe9810ebca0de4d4658d3ceb8e0fe4c066aba3bcc48b105d3bf7e0257d44feceea6596f4d0c59a08402833678f70620f9138dfeb7ded905e4a6d5f05c473d55936652e2a5df43c0cfda7bacaf3087f4524b06cf42157d01539739f7fddec9d58125df31a32eab06c19b71f1d5bf":"a37932f8a7494a942d6f767438e724d6d0c0ef18":"0b5b11ad549863ffa9c51a14a1106c2a72cc8b646e5c7262509786105a984776534ca9b54c1cc64bf2d5a44fd7e8a69db699d5ea52087a4748fd2abc1afed1e5d6f7c89025530bdaa2213d7e030fa55df6f34bcf1ce46d2edf4e3ae4f3b01891a068c9e3a44bbc43133edad6ecb9f35400c4252a5762d65744b99cb9f4c559329f":0

RSASSA-PSS

Signature Example 6_4 (verify)

pkcs1_rsassa_pss_verify:1029:16:"164ca31cff609f3a0e7101b039f2e4fe6dd37519ab98598d179e174996598071f47d3a04559158d7be373cf1aa53f0aa6ef09039e5678c2a4c63900514c8c4f8aaed5de12a5f10b09c311af8c0ffb5b7a297f2efc63b8d6b0510931f0b98e48bf5fc6ec4e7b8db1ffaeb08c38e02adb8f03a48229c99e969431f61cb8c4dc698d1":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"337d25fe9810ebca0de4d4658d3ceb8e0fe4c066aba3bcc48b105d3bf7e0257d44feceea6596f4d0c59a08402833678f70620f9138dfeb7ded905e4a6d5f05c473d55936652e2a5df43c0cfda7bacaf3087f4524b06cf42157d01539739f7fddec9d58125df31a32eab06c19b71f1d5bf":"a37932f8a7494a942d6f767438e724d6d0c0ef18":"0b5b11ad549863ffa9c51a14a1106c2a72cc8b646e5c7262509786105a984776534ca9b54c1cc64bf2d5a44fd7e8a69db699d5ea52087a4748fd2abc1afed1e5d6f7c89025530bdaa2213d7e030fa55df6f34bcf1ce46d2edf4e3ae4f3b01891a068c9e3a44bbc43133edad6ecb9f35400c4252a5762d65744b99cb9f4c559329f":0

RSASSA-PSS

Signature Example 6_5

pkcs1_rsassa_pss_sign:1029:16:"04f0548c9626ab1ebf1244934741d99a06220efa2a5856aa0e75730b2ec96adc86be894fa2803b53a5e85d276acbd29ab823f80a7391bb54a5051672fb04eeb543":16:"0483e0ae47915587743ff345362b555d3962d98bb6f15f848b4c92b1771ca8ed107d8d3ee65ec44517dd0faa481a387e902f7a2e747c269e7ea44480bc538b8e5b":16:"164ca31cff609f3a0e7101b039f2e4fe6dd37519ab98598d179e174996598071f47d3a04559158d7be373cf1aa53f0aa6ef09039e5678c2a4c63900514c8c4f8aaed5de12a5f10b09c311af8c0ffb5b7a297f2efc63b8d6b0510931f0b98e48bf5fc6ec4e7b8db1ffaeb08c38e02adb8f03a48229c99e969431f61cb8c4dc698d1":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"84ec502b072e8287789d8f9235829ea3b187afd4d4c785611bda5f9eb3cb96717efa7007227f1c08cbcb972e667235e0fb7d431a6570326d2ecce35adb373dc753b3be5f829b89175493193fab16badb41371b3aac0ae670076f24bef420c135add7cee8d35fbc944d79fafb9e307a13b0f556cb654a06f973ed22672330197ef5a748bf826a5db2383a25364b686b9372bb2339aeb1ac9e9889327d016f1670776db06201adbdcaf8a5e3b74e108b73":"7b790c1d62f7b84e94df6af28917cf571018110e":"02d71fa9b53e4654fefb7f08385cf6b0ae3a817942ebf66c35ac67f0b069952a3ce9c7e1f1b02e480a9500836de5d64cdb7ecde04542f7a79988787e24c2ba05f5fd482c023ed5c30e04839dc44bed2a3a3a4fee01113c891a47d32eb8025c28cb050b5cdb576c70fe76ef523405c08417faf350b037a43c379339fcb18d3a356b":0

RSASSA-PSS

Signature Example 6_5 (verify)

pkcs1_rsassa_pss_verify:1029:16:"164ca31cff609f3a0e7101b039f2e4fe6dd37519ab98598d179e174996598071f47d3a04559158d7be373cf1aa53f0aa6ef09039e5678c2a4c63900514c8c4f8aaed5de12a5f10b09c311af8c0ffb5b7a297f2efc63b8d6b0510931f0b98e48bf5fc6ec4e7b8db1ffaeb08c38e02adb8f03a48229c99e969431f61cb8c4dc698d1":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"84ec502b072e8287789d8f9235829ea3b187afd4d4c785611bda5f9eb3cb96717efa7007227f1c08cbcb972e667235e0fb7d431a6570326d2ecce35adb373dc753b3be5f829b89175493193fab16badb41371b3aac0ae670076f24bef420c135add7cee8d35fbc944d79fafb9e307a13b0f556cb654a06f973e

d22672330197ef5a748bf826a5db2383a25364b686b9372bb2339aeb1ac9e9889327d016f1670776db06201adbdcaf8a5e3b74e108b73":"7b790c1d62f7b84e94df6af28917cf571018110e":"02d71fa9b53e4654fefb7f08385cf6b0ae3a817942ebf66c35ac67f0b069952a3ce9c7e1f1b02e480a9500836de5d64cdb7ecde04542f7a79988787e24c2ba05f5fd482c023ed5c30e04839dc44bed2a3a3a4fee01113c891a47d32eb8025c28cb050b5cdb576c70fe76ef523405c08417faf350b037a43c379339fcb18d3a356b":0

RSASSA-PSS

Signature Example 6_6

pkcs1_rsassa_pss_sign:1029:16:"04f0548c9626ab1ebf1244934741d99a06220efa2a5856aa0e75730b2ec96adc86be894fa2803b53a5e85d276acbd29ab823f80a7391bb54a5051672fb04eeb543":16:"0483e0ae47915587743ff345362b555d3962d98bb6f15f848b4c92b1771ca8ed107d8d3ee65ec44517dd0faa481a387e902f7a2e747c269e7ea44480bc538b8e5b":16:"164ca31cff609f3a0e7101b039f2e4fe6dd37519ab98598d179e174996598071f47d3a04559158d7be373cf1aa53f0aa6ef09039e5678c2a4c63900514c8c4f8aaed5de12a5f10b09c311af8c0ffb5b7a297f2efc63b8d6b0510931f0b98e48bf5fc6ec4e7b8db1ffaeb08c38e02adb8f03a48229c99e969431f61cb8c4dc698d1":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"9906d89f97a9fdedd3ccd824db687326f30f00aa25a7fca2afcb3b0f86cd41e73f0e8ff7d2d83f59e28ed31a5a0d551523374de22e4c7e8ff568b386ee3dc41163f10bf67bb006261c9082f9af90bf1d9049a6b9fae71c7f84fbe6e55f02789de774f230f115026a4b4e96c55b04a95da3aacbb2cece8f81764a1f1c99515411087cf7d34aeded0932c183":"fbbe059025b69b89fb14ae2289e7aaafe60c0fcd":"0a40a16e2fe2b38d1df90546167cf9469c9e3c3681a3442b4b2c2f581deb385ce99fc6188bb02a841d56e76d301891e24560550fcc2a26b55f4ccb26d837d350a154bcaca8392d98fa67959e9727b78cad03269f56968fc56b68bd679926d83cc9cb215550645ccda31c760ff35888943d2d8a1d351e81e5d07b86182e751081ef":0

RSASSA-PSS

Signature Example 6_6 (verify)

pkcs1_rsassa_pss_verify:1029:16:"164ca31cff609f3a0e7101b039f2e4fe6dd37519ab98598d179e174996598071f47d3a04559158d7be373cf1aa53f0aa6ef09039e5678c2a4c63900514c8c4f8aaed5de12a5f10b09c311af8c0ffb5b7a297f2efc63b8d6b0510931f0b98e48bf5fc6ec4e7b8db1ffaeb08c38e02adb8f03a48229c99e969431f61cb8c4dc698d1":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"9906d89f97a9fdedd3ccd824db687326f30f00aa25a7fca2afcb3b0f86cd41e73f0e8ff7d2d83f59e28ed31a5a0d551523374de22e4c7e8ff568b386ee3dc41163f10bf67bb006261c9082f9af90bf1d9049a6b9fae71c7f84fbe6e55f02789de774f230f115026a4b4e96c55b04a95da3aacbb2cece8f81764a1f1c99515411087cf7d34aeded0932c183":"fbbe059025b69b89fb14ae2289e7aaafe60c0fcd":"0a40a16e2fe2b38d1df90546167cf9469c9e3c3681a3442b4b2c2f581deb385ce99fc6188bb02a841d56e76d301891e24560550fcc2a26b55f4ccb26d837d350a154bcaca8392d98fa67959e9727b78cad03269f56968fc56b68bd679926d83cc9cb215550645ccda31c760ff35888943d2d8a1d351e81e5d07b86182e751081ef":0

RSASSA-PSS

Signature Example 7_1

pkcs1_rsassa_pss_sign:1030:16:"07eefb424b0e3a40e4208ee5afb280b22317308114dde0b4b64f730184ec68da6ce2867a9f48ed7726d5e2614ed04a5410736c8c714ee702474298c6292af07535":16:"070830dbf947eac0228de26314b59b66994cc60e8360e75d3876298f8f8a7d141da064e5ca026a973e28f254738cee669c721b034cb5f8e244dadd7cd1e159d547":16:"37c9da4a66c8c408b8da27d0c9d79f8ccb1eafc1d2fe48746d940b7c4ef5dee18ad12647cefaa0c4b3188b221c515386759b93f02024b25ab9242f8357d8f3fd49640ee5e643eaf6c64deefa7089727c8ff03993333915c6ef21bf5975b6e50d118b51008ec33e9f01a0a545a10a836a43ddbca9d8b5c5d3548022d7064ea29ab3":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"9ead0e01945640674eb41cad435e2374eaefa8ad7197d97913c44957d8d83f40d76ee60e39bf9c0f9eaf3021421a074d1ade962c6e9d3dc3bb174fe4dfe652b09115495b8fd2794174020a0602b5ca51848cfc96ce5eb57fc0a2adc1dda36a7cc452641a14911b37e45bfa11daa5c7ecdb74f6d0100d1d3e39e752800e203397de0233077b9a88855537fae927f924380d780f98e18dcff39c5ea741b17d6fdd1885bc9d581482d771ceb562d78a8bf88f0c75b11363e5e36cd479ceb0545f9da84203e0e6e508375cc9e844b88b7ac7a0a201ea0f1bee9a2c577920ca02c01b9d8320

e974a56f4efb5763b96255abbf8037bf1802cf018f56379493e569a9":"b7867a59958cb54328f8775e6546ec06d27eaa50":"187f390723c8902591f0154bae6d4ecbffe067f0e8b795476ea4f4d51ccc810520bb3ca9bca7d0b1f2ea8a17d873fa27570acd642e3808561cb9e975ccfd80b23dc5771cdb3306a5f23159dacbd3aa2db93d46d766e09ed15d900ad897a8d274dc26b47e994a27e97e2268a766533ae4b5e42a2fcaf755c1c4794b294c60555823":0

RSASSA-PSS
Signature Example 7_1 (verify)
pkcs1_rsassa_pss_verify:1030:16:"37c9da4a66c8c408b8da27d0c9d79f8ccb1eafc1d2fe48746d940b7c4ef5dee18ad12647cefaa0c4b3188b221c515386759b93f02024b25ab9242f8357d8f3fd49640ee5e643eaf6c64deefa7089727c8ff03993333915c6ef21bf5975b6e50d118b51008ec33e9f01a0a545a10a836a43ddbca9d8b5c5d3548022d7064ea29ab3":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"9ead0e01945640674eb41cad435e2374eaefa8ad7197d97913c44957d8d83f40d76ee60e39bf9c0f9eaf3021421a074d1ade962c6e9d3dc3bb174fe4dfe652b09115495b8fd2794174020a0602b5ca51848cfc96ce5eb57fc0a2adc1dda36a7cc452641a14911b37e45bfa11daa5c7ecdb74f6d0100d1d3e39e752800e203397de0233077b9a88855537fae927f924380d780f98e18dcff39c5ea741b17d6fdd1885bc9d581482d771ceb562d78a8bf88f0c75b11363e5e36cd479ceb0545f9da84203e0e6e508375cc9e844b88b7ac7a0a201ea0f1bee9a2c577920ca02c01b9d8320e974a56f4efb5763b96255abbf8037bf1802cf018f56379493e569a9":"b7867a59958cb54328f8775e6546ec06d27eaa50":"187f390723c8902591f0154bae6d4ecbffe067f0e8b795476ea4f4d51ccc810520bb3ca9bca7d0b1f2ea8a17d873fa27570acd642e3808561cb9e975ccfd80b23dc5771cdb3306a5f23159dacbd3aa2db93d46d766e09ed15d900ad897a8d274dc26b47e994a27e97e2268a766533ae4b5e42a2fcaf755c1c4794b294c60555823":0

RSASSA-PSS
Signature Example 7_2
pkcs1_rsassa_pss_sign:1030:16:"07eefb424b0e3a40e4208ee5afb280b22317308114dde0b4b64f730184ec68da6ce2867a9f48ed7726d5e2614ed04a5410736c8c714ee702474298c6292af07535":16:"070830dbf947eac0228de26314b59b66994cc60e8360e75d3876298f8f8a7d141da064e5ca026a973e28f254738cee669c721b034cb5f8e244dadd7cd1e159d547":16:"37c9da4a66c8c408b8da27d0c9d79f8ccb1eafc1d2fe48746d940b7c4ef5dee18ad12647cefaa0c4b3188b221c515386759b93f02024b25ab9242f8357d8f3fd49640ee5e643eaf6c64deefa7089727c8ff03993333915c6ef21bf5975b6e50d118b51008ec33e9f01a0a545a10a836a43ddbca9d8b5c5d3548022d7064ea29ab3":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"8d80d2d08dbd19c154df3f14673a14bd03735231f24e86bf153d0e69e74cbff7b1836e664de83f680124370fc0f96c9b65c07a366b644c4ab3":"0c09582266df086310821ba7e18df64dfee6de09":"10fd89768a60a67788abb5856a787c8561f3edcf9a83e898f7dc87ab8cce79429b43e56906941a886194f137e591fe7c339555361fbbe1f24feb2d4bcdb80601f3096bc9132deea60ae13082f44f9ad41cd628936a4d51176e42fc59cb76db815ce5ab4db99a104aafea68f5d330329ebf258d4ede16064bd1d00393d5e1570eb8":0

RSASSA-PSS
Signature Example 7_2 (verify)
pkcs1_rsassa_pss_verify:1030:16:"37c9da4a66c8c408b8da27d0c9d79f8ccb1eafc1d2fe48746d940b7c4ef5dee18ad12647cefaa0c4b3188b221c515386759b93f02024b25ab9242f8357d8f3fd49640ee5e643eaf6c64deefa7089727c8ff03993333915c6ef21bf5975b6e50d118b51008ec33e9f01a0a545a10a836a43ddbca9d8b5c5d3548022d7064ea29ab3":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"8d80d2d08dbd19c154df3f14673a14bd03735231f24e86bf153d0e69e74cbff7b1836e664de83f680124370fc0f96c9b65c07a366b644c4ab3":"0c09582266df086310821ba7e18df64dfee6de09":"10fd89768a60a67788abb5856a787c8561f3edcf9a83e898f7dc87ab8cce79429b43e56906941a886194f137e591fe7c339555361fbbe1f24feb2d4bcdb80601f3096bc9132deea60ae13082f44f9ad41cd628936a4d51176e42fc59cb76db815ce5ab4db99a104aafea68f5d330329ebf258d4ede16064bd1d00393d5e1570eb8":0

RSASSA-PSS Signature Example 7_3
pkcs1_rsassa_pss_sign:1030:16:"07eefb424b0e3a40e4208ee5afb280b22317308114dde0b4b64f730184ec68da6ce2867a9f48ed7726d5e2614ed04a5410736c8c714ee702474298c6292af07535":16:"070830dbf947eac0228de26314b59b

66994cc60e8360e75d3876298f8f8a7d141da064e5ca026a973e28f254738cee669c721b034cb5f8e244dadd7cd1e159d547":16:"37c9da4a66c8c408b8da27d0c9d79f8ccb1eafc1d2fe48746d940b7c4ef5dee18ad12647cefaa0c4b3188b221c515386759b93f02024b25ab9242f8357d8f3fd49640ee5e643eaf6c64deefa7089727c8ff03993333915c6ef21bf5975b6e50d118b51008ec33e9f01a0a545a10a836a43ddbca9d8b5c5d3548022d7064ea29ab3":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"808405cdfc1a58b9bb0397c720722a81fffb76278f335917ef9c473814b3e016ba2973cd2765f8f3f82d6cc38aa7f8551827fe8d1e3884b7e61c94683b8f82f1843bdae2257eeec9812ad4c2cf283c34e0b0ae0fe3cb990cf88f2ef9":"28039dcfe106d3b8296611258c4a56651c9e92dd":"2b31fde99859b977aa09586d8e274662b25a2a640640b457f594051cb1e7f7a911865455242926cf88fe80dfa3a75ba9689844a11e634a82b075afbd69c12a0df9d25f84ad4945df3dc8fe90c3cefdf26e95f0534304b5bdba20d3e5640a2ebfb898aac35ae40f26fce5563c2f9f24f3042af76f3c7072d687bbfb959a88460af1":0

RSASSA-PSS
Signature Example 7_3 (verify)
pkcs1_rsassa_pss_verify:1030:16:"37c9da4a66c8c408b8da27d0c9d79f8ccb1eafc1d2fe48746d940b7c4ef5dee18ad12647cefaa0c4b3188b221c515386759b93f02024b25ab9242f8357d8f3fd49640ee5e643eaf6c64deefa7089727c8ff03993333915c6ef21bf5975b6e50d118b51008ec33e9f01a0a545a10a836a43ddbca9d8b5c5d3548022d7064ea29ab3":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"808405cdfc1a58b9bb0397c720722a81fffb76278f335917ef9c473814b3e016ba2973cd2765f8f3f82d6cc38aa7f8551827fe8d1e3884b7e61c94683b8f82f1843bdae2257eeec9812ad4c2cf283c34e0b0ae0fe3cb990cf88f2ef9":"28039dcfe106d3b8296611258c4a56651c9e92dd":"2b31fde99859b977aa09586d8e274662b25a2a640640b457f594051cb1e7f7a911865455242926cf88fe80dfa3a75ba9689844a11e634a82b075afbd69c12a0df9d25f84ad4945df3dc8fe90c3cefdf26e95f0534304b5bdba20d3e5640a2ebfb898aac35ae40f26fce5563c2f9f24f3042af76f3c7072d687bbfb959a88460af1":0

RSASSA-PSS Signature Example 7_4
pkcs1_rsassa_pss_sign:1030:16:"07eefb424b0e3a40e4208ee5afb280b22317308114dde0b4b64f730184ec68da6ce2867a9f48ed7726d5e2614ed04a5410736c8c714ee702474298c6292af07535":16:"070830dbf947eac0228de26314b59b66994cc60e8360e75d3876298f8f8a7d141da064e5ca026a973e28f254738cee669c721b034cb5f8e244dadd7cd1e159d547":16:"37c9da4a66c8c408b8da27d0c9d79f8ccb1eafc1d2fe48746d940b7c4ef5dee18ad12647cefaa0c4b3188b221c515386759b93f02024b25ab9242f8357d8f3fd49640ee5e643eaf6c64deefa7089727c8ff03993333915c6ef21bf5975b6e50d118b51008ec33e9f01a0a545a10a836a43ddbca9d8b5c5d3548022d7064ea29ab3":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"f337b9bad937de22a1a052dff11134a8ce26976202981939b91e0715ae5e609649da1adfcef3f4cca59b238360e7d1e496c7bf4b204b5acff9bbd6166a1d87a36ef2247373751039f8a800b8399807b3a85f44893497c0d05fb7017b82228152de6f25e6116dcc7503c786c875c28f3aa607e94ab0f19863ab1b5073770b0cd5f533acde30c6fb953cf3da680264e30fc11bff9a19bffab4779b6223c3fb3fe0f71abade4eb7c09c41e24c22d23fa148e6a173feb63984d1bc6ee3a02d915b752ceaf92a3015eceb38ca586c6801b37c34cefb2cff25ea23c08662dcab26a7a93a285d05d3044c":"a77821ebbbef24628e4e12e1d0ea96de398f7b0f":"32c7ca38ff26949a15000c4ba04b2b13b35a3810e568184d7ecabaa166b7ffabddf2b6cf4ba07124923790f2e5b1a5be040aea36fe132ec130e1f10567982d17ac3e89b8d26c3094034e762d2e031264f01170beecb3d1439e05846f25458367a7d9c02060444672671e64e877864559ca19b2074d588a281b5804d23772fbbe19":0

RSASSA-PSS
Signature Example 7_4 (verify)
pkcs1_rsassa_pss_verify:1030:16:"37c9da4a66c8c408b8da27d0c9d79f8ccb1eafc1d2fe48746d940b7c4ef5dee18ad12647cefaa0c4b3188b221c515386759b93f02024b25ab9242f8357d8f3fd49640ee5e643eaf6c64deefa7089727c8ff03993333915c6ef21bf5975b6e50d118b51008ec33e9f01a0a545a10a836a43ddbca9d8b5c5d3548022d7064ea29ab3":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"f337b9bad937de22a1a052dff11134a8ce26976202981939b91e0715ae5e609649da1adfcef3f4cca59b238360e7d1e496c7bf4b204b5acff9bbd6166a1d87a36ef2247373751039f8a800b8399807b3a85f44893497c0d05fb7017b82228152de6f25e6116dcc7503c786c875c28f3aa607e94ab0f19863a

b1b5073770b0cd5f533acde30c6fb953cf3da680264e30fc11bff9a19bffab4779b6223c3fb3fe0f71abade4eb7c09c41e24c22d23fa148e6a173feb63984d1bc6ee3a02d915b752ceaf92a3015eceb38ca586c6801b37c34cefb2cff25ea23c08662dcab26a7a93a285d05d3044c":"a77821ebbbef24628e4e12e1d0ea96de398f7b0f":"32c7ca38ff26949a15000c4ba04b2b13b35a3810e568184d7ecabaa166b7ffabddf2b6cf4ba07124923790f2e5b1a5be040aea36fe132ec130e1f10567982d17ac3e89b8d26c3094034e762d2e031264f01170beecb3d1439e05846f25458367a7d9c02060444672671e64e877864559ca19b2074d588a281b5804d23772fbbe19":0

RSASSA-PSS
Signature Example 7_5
pkcs1_rsassa_pss_sign:1030:16:"07eefb424b0e3a40e4208ee5afb280b22317308114dde0b4b64f730184ec68da6ce2867a9f48ed7726d5e2614ed04a5410736c8c714ee702474298c6292af07535":16:"070830dbf947eac0228de26314b59b66994cc60e8360e75d3876298f8f8a7d141da064e5ca026a973e28f254738cee669c721b034cb5f8e244dadd7cd1e159d547":16:"37c9da4a66c8c408b8da27d0c9d79f8ccb1eafc1d2fe48746d940b7c4ef5dee18ad12647cefaa0c4b3188b221c515386759b93f02024b25ab9242f8357d8f3fd49640ee5e643eaf6c64deefa7089727c8ff03993333915c6ef21bf5975b6e50d118b51008ec33e9f01a0a545a10a836a43ddbca9d8b5c5d3548022d7064ea29ab3":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"45013cebafd960b255476a8e2598b9aa32efbe6dc1f34f4a498d8cf5a2b4548d08c55d5f95f7bcc9619163056f2d58b52fa032":"9d5ad8eb452134b65dc3a98b6a73b5f741609cd6":"07eb651d75f1b52bc263b2e198336e99fbebc4f332049a922a10815607ee2d989db3a4495b7dccd38f58a211fb7e193171a3d891132437ebca44f318b280509e52b5fa98fcce8205d9697c8ee4b7ff59d4c59c79038a1970bd2a0d451ecdc5ef11d9979c9d35f8c70a6163717607890d586a7c6dc01c79f86a8f28e85235f8c2f1":0

RSASSA-PSS
Signature Example 7_5 (verify)
pkcs1_rsassa_pss_verify:1030:16:"37c9da4a66c8c408b8da27d0c9d79f8ccb1eafc1d2fe48746d940b7c4ef5dee18ad12647cefaa0c4b3188b221c515386759b93f02024b25ab9242f8357d8f3fd49640ee5e643eaf6c64deefa7089727c8ff03993333915c6ef21bf5975b6e50d118b51008ec33e9f01a0a545a10a836a43ddbca9d8b5c5d3548022d7064ea29ab3":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"45013cebafd960b255476a8e2598b9aa32efbe6dc1f34f4a498d8cf5a2b4548d08c55d5f95f7bcc9619163056f2d58b52fa032":"9d5ad8eb452134b65dc3a98b6a73b5f741609cd6":"07eb651d75f1b52bc263b2e198336e99fbebc4f332049a922a10815607ee2d989db3a4495b7dccd38f58a211fb7e193171a3d891132437ebca44f318b280509e52b5fa98fcce8205d9697c8ee4b7ff59d4c59c79038a1970bd2a0d451ecdc5ef11d9979c9d35f8c70a6163717607890d586a7c6dc01c79f86a8f28e85235f8c2f1":0

RSASSA-PSS
Signature Example 7_6
pkcs1_rsassa_pss_sign:1030:16:"07eefb424b0e3a40e4208ee5afb280b22317308114dde0b4b64f730184ec68da6ce2867a9f48ed7726d5e2614ed04a5410736c8c714ee702474298c6292af07535":16:"070830dbf947eac0228de26314b59b66994cc60e8360e75d3876298f8f8a7d141da064e5ca026a973e28f254738cee669c721b034cb5f8e244dadd7cd1e159d547":16:"37c9da4a66c8c408b8da27d0c9d79f8ccb1eafc1d2fe48746d940b7c4ef5dee18ad12647cefaa0c4b3188b221c515386759b93f02024b25ab9242f8357d8f3fd49640ee5e643eaf6c64deefa7089727c8ff03993333915c6ef21bf5975b6e50d118b51008ec33e9f01a0a545a10a836a43ddbca9d8b5c5d3548022d7064ea29ab3":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"2358097086c899323e75d9c90d0c09f12d9d54edfbdf70a9c2eb5a04d8f36b9b2bdf2aabe0a5bda1968937f9d6ebd3b6b257efb3136d4131f9acb59b85e2602c2a3fcdc835494a1f4e5ec18b226c80232b36a75a45fdf09a7ea9e98efbde1450d1194bf12e15a4c5f9eb5c0bce5269e0c3b28cfab655d81a61a20b4be2f54459bb25a0db94c52218be109a7426de83014424789aaa90e5056e632a698115e282c1a56410f26c2072f193481a9dcd880572005e64f4082ecf":"3f2efc595880a7d47fcf3cba04983ea54c4b73fb":"18da3cdcfe79bfb77fd9c32f377ad399146f0a8e8106202233271a6e3ed3248903f5cdc92dc79b55d3e11615aa056a795853792a3998c349ca5c457e8ca7d29d796aa24f83491709befcfb1510ea513c92829a3f00b104f655634f320752e130ec0ccf6754ff893db302932bb025eb60e87822598fc619e0e981737a9a4c4152d33":0

RSASSA-PSS
Signature Example 7_6 (verify)
pkcs1_rsassa_pss_verify:1030:16:"37c9da4a66c8c408b8da27d0c9d79f8ccb1eafc1d2fe48746d940b7c4ef5dee18ad1
2647cefaa0c4b3188b221c515386759b93f02024b25ab9242f8357d8f3fd49640ee5e643eaf6c64deefa7089727c8ff039
93333915c6ef21bf5975b6e50d118b51008ec33e9f01a0a545a10a836a43ddbca9d8b5c5d3548022d7064ea29ab3":16:
"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"2358097086c899323e75d9c90d0c09f12d9d54edfbdf7
0a9c2eb5a04d8f36b9b2bdf2aabe0a5bda1968937f9d6ebd3b6b257efb3136d4131f9acb59b85e2602c2a3fcdc835494a
1f4e5ec18b226c80232b36a75a45fdf09a7ea9e98efbde1450d1194bf12e15a4c5f9eb5c0bce5269e0c3b28cfab655d81a
61a20b4be2f54459bb25a0db94c52218be109a7426de83014424789aaa90e5056e632a698115e282c1a56410f26c2072
f193481a9dcd880572005e64f4082ecf":"3f2efc595880a7d47fcf3cba04983ea54c4b73fb":"18da3cdcfe79bfb77fd9c32
f377ad399146f0a8e810620233271a6e3ed3248903f5cdc92dc79b55d3e11615aa056a795853792a3998c349ca5c457e
8ca7d29d796aa24f83491709befcfb1510ea513c92829a3f00b104f655634f320752e130ec0ccf6754ff893db302932bb0
25eb60e87822598fc619e0e981737a9a4c4152d33":0

RSASSA-PSS
Signature Example 8_1
pkcs1_rsassa_pss_sign:1031:16:"08dad7f11363faa623d5d6d5e8a319328d82190d7127d2846c439b0ab72619b0a43a
95320e4ec34fc3a9cea876422305bd76c5ba7be9e2f410c8060645a1d29edb":16:"0847e732376fc7900f898ea82eb2b0
fc418565fdae62f7d9ec4ce2217b97990dd272db157f99f63c0dcbb9fbacdbd4c4dadb6df67756358ca4174825b48f497
06d":16:"495370a1fb18543c16d3631e3163255df62be6eee890d5f25509e4f778a8ea6fbbbcdf85dff64e0d972003ab36
81fbba6dd41fd541829b2e582de9f2a4a4e0a2d0900bef4753db3cee0ee06c7dfae8b1d53b5953218f9cceea695b08668e
deaadced9463b1d790d5ebf27e9115b46cad4d9a2b8efab0561b0810344739ada0733f":16:"010001":MBEDTLS_MD
_SHA1:MBEDTLS_MD_SHA1:"81332f4be62948415ea1d899792eeacf6c6e1db1da8be13b5cea41db2fed467092e1f
f398914c714259775f595f8547f735692a575e6923af78f22c6997ddb90fb6f72d7bb0dd5744a31decd3dc3685849836e
d34aec596304ad11843c4f88489f209735f5fb7fdaf7cec8addc5818168f880acbf490d51005b7a8e84e43e54287977571
dd99eea4b161eb2df1f5108f12a4142a83322edb05a75487a3435c9a78ce53ed93bc550857d7a9fb":"1d65491d79c864
b373009be6f6f2467bac4c78fa":"0262ac254bfa77f3c1aca22c5179f8f040422b3c5bafd40a8f21cf0fa5a667ccd5993d4
2dbafb409c520e25fce2b1ee1e716577f1efa17f3da28052f40f0419b23106d7845aaf01125b698e7a4dfe92d3967bb00c
4d0d35ba3552ab9a8b3eef07c7fecdbc5424ac4db1e20cb37d0b2744769940ea907e17fbbca673b20522380c5":0

RSASSA-PSS
Signature Example 8_1 (verify)
pkcs1_rsassa_pss_verify:1031:16:"495370a1fb18543c16d3631e3163255df62be6eee890d5f25509e4f778a8ea6fbbbc
df85dff64e0d972003ab3681fbba6dd41fd541829b2e582de9f2a4a4e0a2d0900bef4753db3cee0ee06c7dfae8b1d53b59
53218f9cceea695b08668edeaadced9463b1d790d5ebf27e9115b46cad4d9a2b8efab0561b0810344739ada0733f":16:"
010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"81332f4be62948415ea1d899792eeacf6c6e1db1da8be13
b5cea41db2fed467092e1ff398914c714259775f595f8547f735692a575e6923af78f22c6997ddb90fb6f72d7bb0dd5744
a31decd3dc3685849836ed34aec596304ad11843c4f88489f209735f5fb7fdaf7cec8addc5818168f880acbf490d51005b
7a8e84e43e54287977571dd99eea4b161eb2df1f5108f12a4142a83322edb05a75487a3435c9a78ce53ed93bc550857d
7a9fb":"1d65491d79c864b373009be6f6f2467bac4c78fa":"0262ac254bfa77f3c1aca22c5179f8f040422b3c5bafd40a8
f21cf0fa5a667ccd5993d42dbafb409c520e25fce2b1ee1e716577f1efa17f3da28052f40f0419b23106d7845aaf01125b6
98e7a4dfe92d3967bb00c4d0d35ba3552ab9a8b3eef07c7fecdbc5424ac4db1e20cb37d0b2744769940ea907e17fbbca6
73b20522380c5":0

RSASSA-PSS
Signature

Example 8_2

pkcs1_rsassa_pss_sign:1031:16:"08dad7f11363faa623d5d6d5e8a319328d82190d7127d2846c439b0ab72619b0a43a95320e4ec34fc3a9cea876422305bd76c5ba7be9e2f410c8060645a1d29edb":16:"0847e732376fc7900f898ea82eb2b0fc418565fdae62f7d9ec4ce2217b97990dd272db157f99f63c0dcbb9fbacdbd4c4dadb6df67756358ca4174825b48f49706d":16:"495370a1fb18543c16d3631e3163255df62be6eee890d5f25509e4f778a8ea6fbbbcdf85dff64e0d972003ab3681fbba6dd41fd541829b2e582de9f2a4a4e0a2d0900bef4753db3cee0ee06c7dfae8b1d53b5953218f9cceea695b08668edeaadced9463b1d790d5ebf27e9115b46cad4d9a2b8efab0561b0810344739ada0733f":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"e2f96eaf0e05e7ba326ecca0ba7fd2f7c02356f3cede9d0faabf4fcc8e60a973e5595fd9ea08":"435c098aa9909eb2377f1248b091b68987ff1838":"2707b9ad5115c58c94e932e8ec0a280f56339e44a1b58d4ddcff2f312e5f34dcfe39e89c6a94dcee86dbbdae5b79ba4e0819a9e7bfd9d982e7ee6c86ee68396e8b3a14c9c8f34b178eb741f9d3f121109bf5c8172fada2e768f9ea1433032c004a8aa07eb990000a48dc94c8bac8aabe2b09b1aa46c0a2aa0e12f63fbba775ba7e":0

RSASSA-PSS

Signature Example 8_2 (verify)

pkcs1_rsassa_pss_verify:1031:16:"495370a1fb18543c16d3631e3163255df62be6eee890d5f25509e4f778a8ea6fbbbcdf85dff64e0d972003ab3681fbba6dd41fd541829b2e582de9f2a4a4e0a2d0900bef4753db3cee0ee06c7dfae8b1d53b5953218f9cceea695b08668edeaadced9463b1d790d5ebf27e9115b46cad4d9a2b8efab0561b0810344739ada0733f":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"e2f96eaf0e05e7ba326ecca0ba7fd2f7c02356f3cede9d0faabf4fcc8e60a973e5595fd9ea08":"435c098aa9909eb2377f1248b091b68987ff1838":"2707b9ad5115c58c94e932e8ec0a280f56339e44a1b58d4ddcff2f312e5f34dcfe39e89c6a94dcee86dbbdae5b79ba4e0819a9e7bfd9d982e7ee6c86ee68396e8b3a14c9c8f34b178eb741f9d3f121109bf5c8172fada2e768f9ea1433032c004a8aa07eb990000a48dc94c8bac8aabe2b09b1aa46c0a2aa0e12f63fbba775ba7e":0

RSASSA-PSS Signature Example 8_3

pkcs1_rsassa_pss_sign:1031:16:"08dad7f11363faa623d5d6d5e8a319328d82190d7127d2846c439b0ab72619b0a43a95320e4ec34fc3a9cea876422305bd76c5ba7be9e2f410c8060645a1d29edb":16:"0847e732376fc7900f898ea82eb2b0fc418565fdae62f7d9ec4ce2217b97990dd272db157f99f63c0dcbb9fbacdbd4c4dadb6df67756358ca4174825b48f49706d":16:"495370a1fb18543c16d3631e3163255df62be6eee890d5f25509e4f778a8ea6fbbbcdf85dff64e0d972003ab3681fbba6dd41fd541829b2e582de9f2a4a4e0a2d0900bef4753db3cee0ee06c7dfae8b1d53b5953218f9cceea695b08668edeaadced9463b1d790d5ebf27e9115b46cad4d9a2b8efab0561b0810344739ada0733f":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"e35c6ed98f64a6d5a648fcab8adb16331db32e5d15c74a40edf94c3dc4a4de792d190889f20f1e24ed12054a6b28798fcb42d1c548769b734c96373142092aed277603f4738df4dc1446586d0ec64da4fb60536db2ae17fc7e3c04bbfbbbd907bf117c08636fa16f95f51a6216934d3e34f85030f17bbbc5ba69144058aff081e0b19cf03c17195c5e888ba58f6fe0a02e5c3bda9719a7":"c6ebbe76df0c4aea32c474175b2f136862d04529":"2ad20509d78cf26d1b6c406146086e4b0c91a91c2bd164c87b966b8faa42aa0ca446022323ba4b1a1b89706d7f4c3be57d7b69702d168ab5955ee290356b8c4a29ed467d547ec23cbadf286ccb5863c6679da467fc9324a151c7ec55aac6db4084f82726825cfe1aa421bc64049fb42f23148f9c25b2dc300437c38d428aa75f96":0

RSASSA-PSS

Signature Example 8_3 (verify)

pkcs1_rsassa_pss_verify:1031:16:"495370a1fb18543c16d3631e3163255df62be6eee890d5f25509e4f778a8ea6fbbbcdf85dff64e0d972003ab3681fbba6dd41fd541829b2e582de9f2a4a4e0a2d0900bef4753db3cee0ee06c7dfae8b1d53b5953218f9cceea695b08668edeaadced9463b1d790d5ebf27e9115b46cad4d9a2b8efab0561b0810344739ada0733f":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"e35c6ed98f64a6d5a648fcab8adb16331db32e5d15c74a40edf94c3dc4a4de792d190889f20f1e24ed12054a6b28798fcb42d1c548769b734c96373142092aed277603f4738df4dc1446586d0ec64da4fb60536db2ae17fc7e3c04bbfbbbd907bf117c08636fa16f95f51a6216934d3e34f85030f17bbbc5ba69144058aff081e0b19cf03c17195c5e888ba58f6fe0a02e5c3bda9719a7":"c6ebbe76df0c4aea32c474175b2f136862d0

4529":"2ad20509d78cf26d1b6c406146086e4b0c91a91c2bd164c87b966b8faa42aa0ca446022323ba4b1a1b89706d7f
4c3be57d7b69702d168ab5955ee290356b8c4a29ed467d547ec23cbadf286ccb5863c6679da467fc9324a151c7ec55aa
c6db4084f82726825cfe1aa421bc64049fb42f23148f9c25b2dc300437c38d428aa75f96":0

RSASSA-PSS
Signature Example 8_4
pkcs1_rsassa_pss_sign:1031:16:"08dad7f11363faa623d5d6d5e8a319328d82190d7127d2846c439b0ab72619b0a43a
95320e4ec34fc3a9cea876422305bd76c5ba7be9e2f410c8060645a1d29edb":16:"0847e732376fc7900f898ea82eb2b0
fc418565fdae62f7d9ec4ce2217b97990dd272db157f99f63c0dcbb9fbacdbd4c4dadb6df67756358ca4174825b48f497
06d":16:"495370a1fb18543c16d3631e3163255df62be6eee890d5f25509e4f778a8ea6fbbbcdf85dff64e0d972003ab36
81fbba6dd41fd541829b2e582de9f2a4a4e0a2d0900bef4753db3cee0ee06c7dfae8b1d53b5953218f9cceea695b08668e
deaadced9463b1d790d5ebf27e9115b46cad4d9a2b8efab0561b0810344739ada0733f":16:"010001":MBEDTLS_MD
_SHA1:MBEDTLS_MD_SHA1:"dbc5f750a7a14be2b93e838d18d14a8695e52e8add9c0ac733b8f56d2747e529a0cc
a532dd49b902aefed514447f9e81d16195c2853868cb9b30f7d0d495c69d01b5c5d50b27045db3866c2324a44a110b1
717746de457d1c8c45c3cd2a92970c3d59632055d4c98a41d6e99e2a3ddd5f7f9979ab3cd18f37505d25141de2a1bff17
b3a7dce9419ecc385cf11d72840f19953fd0509251f6cafde2893d0e75c781ba7a5012ca401a4fa99e04b3c3249f926d5a
fe82cc87dab22c3c1b105de48e34ace9c9124e59597ac7ebf8":"021fdcc6ebb5e19b1cb16e9c67f27681657fe20a":"1e2
4e6e58628e5175044a9eb6d837d48af1260b0520e87327de7897ee4d5b9f0df0be3e09ed4dea8c1454ff3423bb08e1793
245a9df8bf6ab3968c8eddc3b5328571c77f091cc578576912dfebd164b9de5454fe0be1c1f6385b328360ce67ec7a05f
6e30eb45c17c48ac70041d2cab67f0a2ae7aafdcc8d245ea3442a6300ccc7":0

RSASSA-PSS
Signature Example 8_4 (verify)
pkcs1_rsassa_pss_verify:1031:16:"495370a1fb18543c16d3631e3163255df62be6eee890d5f25509e4f778a8ea6fbbbc
df85dff64e0d972003ab3681fbba6dd41fd541829b2e582de9f2a4a4e0a2d0900bef4753db3cee0ee06c7dfae8b1d53b59
53218f9cceea695b08668edeaadced9463b1d790d5ebf27e9115b46cad4d9a2b8efab0561b0810344739ada0733f":16:"
010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"dbc5f750a7a14be2b93e838d18d14a8695e52e8add9c0a
c733b8f56d2747e529a0cca532dd49b902aefed514447f9e81d16195c2853868cb9b30f7d0d495c69d01b5c5d50b2704
5db3866c2324a44a110b1717746de457d1c8c45c3cd2a92970c3d59632055d4c98a41d6e99e2a3ddd5f7f9979ab3cd18
f37505d25141de2a1bff17b3a7dce9419ecc385cf11d72840f19953fd0509251f6cafde2893d0e75c781ba7a5012ca401a
4fa99e04b3c3249f926d5afe82cc87dab22c3c1b105de48e34ace9c9124e59597ac7ebf8":"021fdcc6ebb5e19b1cb16e9c
67f27681657fe20a":"1e24e6e58628e5175044a9eb6d837d48af1260b0520e87327de7897ee4d5b9f0df0be3e09ed4dea
8c1454ff3423bb08e1793245a9df8bf6ab3968c8eddc3b5328571c77f091cc578576912dfebd164b9de5454fe0be1c1f6
385b328360ce67ec7a05f6e30eb45c17c48ac70041d2cab67f0a2ae7aafdcc8d245ea3442a6300ccc7":0

RSASSA-PSS
Signature Example 8_5
pkcs1_rsassa_pss_sign:1031:16:"08dad7f11363faa623d5d6d5e8a319328d82190d7127d2846c439b0ab72619b0a43a
95320e4ec34fc3a9cea876422305bd76c5ba7be9e2f410c8060645a1d29edb":16:"0847e732376fc7900f898ea82eb2b0
fc418565fdae62f7d9ec4ce2217b97990dd272db157f99f63c0dcbb9fbacdbd4c4dadb6df67756358ca4174825b48f497
06d":16:"495370a1fb18543c16d3631e3163255df62be6eee890d5f25509e4f778a8ea6fbbbcdf85dff64e0d972003ab36
81fbba6dd41fd541829b2e582de9f2a4a4e0a2d0900bef4753db3cee0ee06c7dfae8b1d53b5953218f9cceea695b08668e
deaadced9463b1d790d5ebf27e9115b46cad4d9a2b8efab0561b0810344739ada0733f":16:"010001":MBEDTLS_MD
_SHA1:MBEDTLS_MD_SHA1:"04dc251be72e88e5723485b6383a637e2fefe07660c519a560b8bc18bdedb86eae23
64ea53ba9dca6eb3d2e7d6b806af42b3e87f291b4a8881d5bf572cc9a85e19c86acb28f098f9da0383c566d3c0f58cfd8f
395dcf602e5cd40e8c7183f714996e2297ef":"c558d7167cbb4508ada042971e71b1377eea4269":"33341ba3576a130a
50e2a5cf8679224388d5693f5accc235ac95add68e5eb1eec31666d0ca7a1cda6f70a1aa762c05752a51950cdb8af3c537
9f18cfe6b5bc55a4648226a15e912ef19ad77adeea911d67cfefd69ba43fa4119135ff642117ba985a7e0100325e9519f1

ca6a9216bda055b5785015291125e90dcd07a2ca9673ee":0

RSASSA-PSS
Signature Example 8_5 (verify)
pkcs1_rsassa_pss_verify:1031:16:"495370a1fb18543c16d3631e3163255df62be6eee890d5f25509e4f778a8ea6fbbbc
df85dff64e0d972003ab3681fbba6dd41fd541829b2e582de9f2a4a4e0a2d0900bef4753db3cee0ee06c7dfae8b1d53b59
53218f9cceea695b08668edeaadced9463b1d790d5ebf27e9115b46cad4d9a2b8efab0561b0810344739ada0733f":16:"
010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"04dc251be72e88e5723485b6383a637e2fefe07660c519
a560b8bc18bdedb86eae2364ea53ba9dca6eb3d2e7d6b806af42b3e87f291b4a8881d5bf572cc9a85e19c86acb28f098f
9da0383c566d3c0f58cfd8f395dcf602e5cd40e8c7183f714996e2297ef":"c558d7167cbb4508ada042971e71b1377eea
4269":"33341ba3576a130a50e2a5cf8679224388d5693f5accc235ac95add68e5eb1eec31666d0ca7a1cda6f70a1aa762
c05752a51950cdb8af3c5379f18cfe6b5bc55a4648226a15e912ef19ad77adeea911d67cfefd69ba43fa4119135ff64211
7ba985a7e0100325e9519f1ca6a9216bda055b5785015291125e90dcd07a2ca9673ee":0

RSASSA-PSS
Signature Example 8_6
pkcs1_rsassa_pss_sign:1031:16:"08dad7f11363faa623d5d6d5e8a319328d82190d7127d2846c439b0ab72619b0a43a
95320e4ec34fc3a9cea876422305bd76c5ba7be9e2f410c8060645a1d29edb":16:"0847e732376fc7900f898ea82eb2b0
fc418565fdae62f7d9ec4ce2217b97990dd272db157f99f63c0dcbb9fbacdbd4c4dadb6df67756358ca4174825b48f497
06d":16:"495370a1fb18543c16d3631e3163255df62be6eee890d5f25509e4f778a8ea6fbbbcdf85dff64e0d972003ab36
81fbba6dd41fd541829b2e582de9f2a4a4e0a2d0900bef4753db3cee0ee06c7dfae8b1d53b5953218f9cceea695b08668e
deaadced9463b1d790d5ebf27e9115b46cad4d9a2b8efab0561b0810344739ada0733f":16:"010001":MBEDTLS_MD
_SHA1:MBEDTLS_MD_SHA1:"0ea37df9a6fea4a8b610373c24cf390c20fa6e2135c400c8a34f5c183a7e8ea4c9ae09
0ed31759f42dc77719cca400ecdcc517acfc7ac6902675b2ef30c509665f3321482fc69a9fb570d15e01c845d0d8e50d2a
24cbf1cf0e714975a5db7b18d9e9e9cb91b5cb16869060ed18b7b56245503f0caf90352b8de81cb5a1d9c6336092f0cd"
:"76fd4e64fdc98eb927a0403e35a084e76ba9f92a":"1ed1d848fb1edb44129bd9b354795af97a069a7a00d0151048593
e0c72c3517ff9ff2a41d0cb5a0ac860d736a199704f7cb6a53986a88bbd8abcc0076a2ce847880031525d449da2ac7835
6374c536e343faa7cba42a5aaa6506087791c06a8e989335aed19bfab2d5e67e27fb0c2875af896c21b6e8e7309d04e4f
6727e69463e":0

RSASSA-PSS
Signature Example 8_6 (verify)
pkcs1_rsassa_pss_verify:1031:16:"495370a1fb18543c16d3631e3163255df62be6eee890d5f25509e4f778a8ea6fbbbc
df85dff64e0d972003ab3681fbba6dd41fd541829b2e582de9f2a4a4e0a2d0900bef4753db3cee0ee06c7dfae8b1d53b59
53218f9cceea695b08668edeaadced9463b1d790d5ebf27e9115b46cad4d9a2b8efab0561b0810344739ada0733f":16:"
010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"0ea37df9a6fea4a8b610373c24cf390c20fa6e2135c400c
8a34f5c183a7e8ea4c9ae090ed31759f42dc77719cca400ecdcc517acfc7ac6902675b2ef30c509665f3321482fc69a9fb
570d15e01c845d0d8e50d2a24cbf1cf0e714975a5db7b18d9e9e9cb91b5cb16869060ed18b7b56245503f0caf90352b8
de81cb5a1d9c6336092f0cd":"76fd4e64fdc98eb927a0403e35a084e76ba9f92a":"1ed1d848fb1edb44129bd9b354795
af97a069a7a00d0151048593e0c72c3517ff9ff2a41d0cb5a0ac860d736a199704f7cb6a53986a88bbd8abcc0076a2ce84
7880031525d449da2ac78356374c536e343faa7cba42a5aaa6506087791c06a8e989335aed19bfab2d5e67e27fb0c2875
af896c21b6e8e7309d04e4f6727e69463e":0

RSASSA-PSS
Signature Example 9_1
pkcs1_rsassa_pss_sign:1536:16:"f8eb97e98df12664eefdb761596a69ddcd0e76daece6ed4bf5a1b50ac086f7928a4d2f
8726a77e515b74da41988f220b1cc87aa1fc810ce99a82f2d1ce821edced794c6941f42c7a1a0b8c4d28c75ec60b65227
9f6154a762aed165d47dee367":16:"ed4d71d0a6e24b93c2e5f6b4bbe05f5fb0afa042d204fe3378d365c2f288b6a8dad7

efe45d153eef40cacc7b81ff934002d108994b94a5e4728cd9c963375ae49965bda55cbf0efed8d6553b4027f2d86208a6
e6b489c176128092d629e49d3d":16:"e6bd692ac96645790403fdd0f5beb8b9bf92ed10007fc365046419dd06c05c5b5
b2f48ecf989e4ce269109979cbb40b4a0ad24d22483d1ee315ad4ccb1534268352691c524f6dd8e6c29d224cf246973ae
c86c5bf6b1401a850d1b9ad1bb8cbcec47b06f0f8c7f45d3fc8f319299c5433ddbc2b3053b47ded2ecd4a4caefd614833d
c8bb622f317ed076b8057fe8de3f84480ad5e83e4a61904a4f248fb397027357e1d30e463139815c6fd4fd5ac5b8172a4
5230ecb6318a04f1455d84e5a8b":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"a88e265855e9d7
ca36c68795f0b31b591cd6587c71d060a0b3f7f3eaef43795922028bc2b6ad467cfc2d7f659c5385aa70ba3672cdde4cfe
4970cc7904601b278872bf51321c4a972f3c95570f3445d4f57980e0f20df54846e6a52c668f1288c03f95006ea32f562
d40d52af9feb32f0fa06db65b588a237b34e592d55cf979f903a642ef64d2ed542aa8c77dc1dd762f45a59303ed75e541c
a271e2b60ca709e44fa0661131e8d5d4163fd8d398566ce26de8730e72f9cca737641c244159420637028df0a18079d6
208ea8b4711a2c750f5":"c0a425313df8d7564bd2434d311523d5257eed80":"586107226c3ce013a7c8f04d1a6a2959
bb4b8e205ba43a27b50f124111bc35ef589b039f5932187cb696d7d9a32c0c38300a5cdda4834b62d2eb240af33f79d1
3dfbf095bf599e0d9686948c1964747b67e89c9aba5cd85016236f566cc5802cb13ead51bc7ca6bef3b94dcbdbb1d5704
69771df0e00b1a8a06777472d2316279edae86474668d4e1efff95f1de61c6020da32ae92bbf16520fef3cf4d88f61121f
24bbd9fe91b59caf1235b2a93ff81fc403addf4ebdea84934a9cdaf8e1a9e":0

RSASSA-PSS

Signature Example 9_1 (verify)

pkcs1_rsassa_pss_verify:1536:16:"e6bd692ac96645790403fdd0f5beb8b9bf92ed10007fc365046419dd06c05c5b5b2
f48ecf989e4ce269109979cbb40b4a0ad24d22483d1ee315ad4ccb1534268352691c524f6dd8e6c29d224cf246973aec8
6c5bf6b1401a850d1b9ad1bb8cbcec47b06f0f8c7f45d3fc8f319299c5433ddbc2b3053b47ded2ecd4a4caefd614833dc8
bb622f317ed076b8057fe8de3f84480ad5e83e4a61904a4f248fb397027357e1d30e463139815c6fd4fd5ac5b8172a452
30ecb6318a04f1455d84e5a8b":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"a88e265855e9d7ca
36c68795f0b31b591cd6587c71d060a0b3f7f3eaef43795922028bc2b6ad467cfc2d7f659c5385aa70ba3672cdde4cfe49
70cc7904601b278872bf51321c4a972f3c95570f3445d4f57980e0f20df54846e6a52c668f1288c03f95006ea32f562d4
0d52af9feb32f0fa06db65b588a237b34e592d55cf979f903a642ef64d2ed542aa8c77dc1dd762f45a59303ed75e541ca2
71e2b60ca709e44fa0661131e8d5d4163fd8d398566ce26de8730e72f9cca737641c244159420637028df0a18079d620
8ea8b4711a2c750f5":"c0a425313df8d7564bd2434d311523d5257eed80":"586107226c3ce013a7c8f04d1a6a2959bb
4b8e205ba43a27b50f124111bc35ef589b039f5932187cb696d7d9a32c0c38300a5cdda4834b62d2eb240af33f79d13df
bf095bf599e0d9686948c1964747b67e89c9aba5cd85016236f566cc5802cb13ead51bc7ca6bef3b94dcbdbb1d570469
771df0e00b1a8a06777472d2316279edae86474668d4e1efff95f1de61c6020da32ae92bbf16520fef3cf4d88f61121f24
bbd9fe91b59caf1235b2a93ff81fc403addf4ebdea84934a9cdaf8e1a9e":0

RSASSA-PSS

Signature Example 9_2

pkcs1_rsassa_pss_sign:1536:16:"f8eb97e98df12664eefdb761596a69ddcd0e76daece6ed4bf5a1b50ac086f7928a4d2f
8726a77e515b74da41988f220b1cc87aa1fc810ce99a82f2d1ce821edced794c6941f42c7a1a0b8c4d28c75ec60b65227
9f6154a762aed165d47dee367":16:"ed4d71d0a6e24b93c2e5f6b4bbe05f5fb0afa042d204fe3378d365c2f288b6a8dad7
efe45d153eef40cacc7b81ff934002d108994b94a5e4728cd9c963375ae49965bda55cbf0efed8d6553b4027f2d86208a6
e6b489c176128092d629e49d3d":16:"e6bd692ac96645790403fdd0f5beb8b9bf92ed10007fc365046419dd06c05c5b5
b2f48ecf989e4ce269109979cbb40b4a0ad24d22483d1ee315ad4ccb1534268352691c524f6dd8e6c29d224cf246973ae
c86c5bf6b1401a850d1b9ad1bb8cbcec47b06f0f8c7f45d3fc8f319299c5433ddbc2b3053b47ded2ecd4a4caefd614833d
c8bb622f317ed076b8057fe8de3f84480ad5e83e4a61904a4f248fb397027357e1d30e463139815c6fd4fd5ac5b8172a4
5230ecb6318a04f1455d84e5a8b":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"c8c9c6af04acda4
14d227ef23e0820c3732c500dc87275e95b0d095413993c2658bc1d988581ba879c2d201f14cb88ced153a01969a7bf0
a7be79c84c1486bc12b3fa6c59871b6827c8ce253ca5fefa8a8c690bf326e8e37cdb96d90a82ebab69f86350e1822e8bd
536a2e":"b307c43b4850a8dac2f15f32e37839ef8c5c0e91":"80b6d643255209f0a456763897ac9ed259d459b49c2887
e5882ecb4434cfd66dd7e1699375381e51cd7f554f2c271704b399d42b4be2540a0eca61951f55267f7c2878c122842da

db28b01bd5f8c025f7e228418a673c03d6bc0c736d0a29546bd67f786d9d692ccea778d71d98c2063b7a71092187a4d3
5af108111d83e83eae46c46aa34277e06044589903788f1d5e7cee25fb485e92949118814d6f2c3ee361489016f327fb5
bc517eb50470bffa1afa5f4ce9aa0ce5b8ee19bf5501b958":0

RSASSA-PSS
Signature Example 9_2 (verify)
pkcs1_rsassa_pss_verify:1536:16:"e6bd692ac96645790403fdd0f5beb8b9bf92ed10007fc365046419dd06c05c5b5b2
f48ecf989e4ce269109979cbb40b4a0ad24d22483d1ee315ad4ccb1534268352691c524f6dd8e6c29d224cf246973aec8
6c5bf6b1401a850d1b9ad1bb8cbcec47b06f0f8c7f45d3fc8f319299c5433ddbc2b3053b47ded2ecd4a4caefd614833dc8
bb622f317ed076b8057fe8de3f84480ad5e83e4a61904a4f248fb397027357e1d30e463139815c6fd4fd5ac5b8172a452
30ecb6318a04f1455d84e5a8b":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"c8c9c6af04acda414
d227ef23e0820c3732c500dc87275e95b0d095413993c2658bc1d988581ba879c2d201f14cb88ced153a01969a7bf0a7
be79c84c1486bc12b3fa6c59871b6827c8ce253ca5fefa8a8c690bf326e8e37cdb96d90a82ebab69f86350e1822e8bd53
6a2e":"b307c43b4850a8dac2f15f32e37839ef8c5c0e91":"80b6d643255209f0a456763897ac9ed259d459b49c2887e5
882ecb4434cfd66dd7e1699375381e51cd7f554f2c271704b399d42b4be2540a0eca61951f55267f7c2878c122842dad
b28b01bd5f8c025f7e228418a673c03d6bc0c736d0a29546bd67f786d9d692ccea778d71d98c2063b7a71092187a4d35
af108111d83e83eae46c46aa34277e06044589903788f1d5e7cee25fb485e92949118814d6f2c3ee361489016f327fb5b
c517eb50470bffa1afa5f4ce9aa0ce5b8ee19bf5501b958":0

RSASSA-PSS
Signature Example 9_3
pkcs1_rsassa_pss_sign:1536:16:"f8eb97e98df12664eefdb761596a69ddcd0e76daece6ed4bf5a1b50ac086f7928a4d2f
8726a77e515b74da41988f220b1cc87aa1fc810ce99a82f2d1ce821edced794c6941f42c7a1a0b8c4d28c75ec60b65227
9f6154a762aed165d47dee367":16:"ed4d71d0a6e24b93c2e5f6b4bbe05f5fb0afa042d204fe3378d365c2f288b6a8dad7
efe45d153eef40cacc7b81ff934002d108994b94a5e4728cd9c963375ae49965bda55cbf0efed8d6553b4027f2d86208a6
e6b489c176128092d629e49d3d":16:"e6bd692ac96645790403fdd0f5beb8b9bf92ed10007fc365046419dd06c05c5b5
b2f48ecf989e4ce269109979cbb40b4a0ad24d22483d1ee315ad4ccb1534268352691c524f6dd8e6c29d224cf246973ae
c86c5bf6b1401a850d1b9ad1bb8cbcec47b06f0f8c7f45d3fc8f319299c5433ddbc2b3053b47ded2ecd4a4caefd614833d
c8bb622f317ed076b8057fe8de3f84480ad5e83e4a61904a4f248fb397027357e1d30e463139815c6fd4fd5ac5b8172a4
5230ecb6318a04f1455d84e5a8b":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"0afad42ccd4fc60
654a55002d228f52a4a5fe03b8bbb08ca82daca558b44dbe1266e50c0e745a36d9d2904e3408abcd1fd569994063f4a7
5cc72f2fee2a0cd893a43af1c5b8b487df0a71610024e4f6ddf9f28ad0813c1aab91bcb3c9064d5ff742deffea657094139
369e5ea6f4a96319a5cc8224145b545062758fefd1fe3409ae169259c6cdfd6b5f2958e314faecbe69d2cace58ee55179a
b9b3e6d1ecc14a557c5febe988595264fc5da1c571462eca798a18a1a4940cdab4a3e92009ccd42e1e947b1314e32238a
2dece7d23a89b5b30c751fd0a4a430d2c548594":"9a2b007e80978bbb192c354eb7da9aedfc74dbf5":"484408f3898cd
5f53483f80819efbf2708c34d27a8b2a6fae8b322f9240237f981817aca1846f1084daa6d7c0795f6e5bf1af59c38e18584
37ce1f7ec419b98c8736adf6dd9a00b1806d2bd3ad0a73775e05f52dfef3a59ab4b08143f0df05cd1ad9d04bececa6daa4
a2129803e200cbc77787caf4c1d0663a6c5987b605952019782caf2ec1426d68fb94ed1d4be816a7ed081b77e6ab330b
3ffc073820fecde3727fcbe295ee61a050a343658637c3fd659cfb63736de32d9f90d3c2f63eca":0

RSASSA-PSS
Signature Example 9_3 (verify)
pkcs1_rsassa_pss_verify:1536:16:"e6bd692ac96645790403fdd0f5beb8b9bf92ed10007fc365046419dd06c05c5b5b2
f48ecf989e4ce269109979cbb40b4a0ad24d22483d1ee315ad4ccb1534268352691c524f6dd8e6c29d224cf246973aec8
6c5bf6b1401a850d1b9ad1bb8cbcec47b06f0f8c7f45d3fc8f319299c5433ddbc2b3053b47ded2ecd4a4caefd614833dc8
bb622f317ed076b8057fe8de3f84480ad5e83e4a61904a4f248fb397027357e1d30e463139815c6fd4fd5ac5b8172a452
30ecb6318a04f1455d84e5a8b":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"0afad42ccd4fc6065
4a55002d228f52a4a5fe03b8bbb08ca82daca558b44dbe1266e50c0e745a36d9d2904e3408abcd1fd569994063f4a75cc

72f2fee2a0cd893a43af1c5b8b487df0a71610024e4f6ddf9f28ad0813c1aab91bcb3c9064d5ff742deffea657094139369
e5ea6f4a96319a5cc8224145b545062758fefd1fe3409ae169259c6cdfd6b5f2958e314faecbe69d2cace58ee55179ab9b
3e6d1ecc14a557c5febe988595264fc5da1c571462eca798a18a1a4940cdab4a3e92009ccd42e1e947b1314e32238a2de
ce7d23a89b5b30c751fd0a4a430d2c548594":"9a2b007e80978bbb192c354eb7da9aedfc74dbf5":"484408f3898cd5f5
3483f80819efbf2708c34d27a8b2a6fae8b322f9240237f981817aca1846f1084daa6d7c0795f6e5bf1af59c38e1858437
ce1f7ec419b98c8736adf6dd9a00b1806d2bd3ad0a73775e05f52dfef3a59ab4b08143f0df05cd1ad9d04bececa6daa4a2
129803e200cbc77787caf4c1d0663a6c5987b605952019782caf2ec1426d68fb94ed1d4be816a7ed081b77e6ab330b3ff
c073820fecde3727fcbe295ee61a050a343658637c3fd659cfb63736de32d9f90d3c2f63eca":0

RSASSA-PSS

Signature Example 9_4

pkcs1_rsassa_pss_sign:1536:16:"f8eb97e98df12664eefdb761596a69ddcd0e76daece6ed4bf5a1b50ac086f7928a4d2f
8726a77e515b74da41988f220b1cc87aa1fc810ce99a82f2d1ce821edced794c6941f42c7a1a0b8c4d28c75ec60b65227
9f6154a762aed165d47dee367":16:"ed4d71d0a6e24b93c2e5f6b4bbe05f5fb0afa042d204fe3378d365c2f288b6a8dad7
efe45d153eef40cacc7b81ff934002d108994b94a5e4728cd9c963375ae49965bda55cbf0efed8d6553b4027f2d86208a6
e6b489c176128092d629e49d3d":16:"e6bd692ac96645790403fdd0f5beb8b9bf92ed10007fc365046419dd06c05c5b5
b2f48ecf989e4ce269109979cbb40b4a0ad24d22483d1ee315ad4ccb1534268352691c524f6dd8e6c29d224cf246973ae
c86c5bf6b1401a850d1b9ad1bb8cbcec47b06f0f8c7f45d3fc8f319299c5433ddbc2b3053b47ded2ecd4a4caefd614833d
c8bb622f317ed076b8057fe8de3f84480ad5e83e4a61904a4f248fb397027357e1d30e463139815c6fd4fd5ac5b8172a4
5230ecb6318a04f1455d84e5a8b":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"1dfd43b46c93db
82629bdae2bd0a12b882ea04c3b465f5cf93023f01059626dbbe99f26bb1be949dddd16dc7f3debb19a194627f0b2244
34df7d8700e9e98b06e360c12fdbe3d19f51c9684eb9089ecbb0a2f0450399d3f59eac7294085d044f5393c6ce737423d
8b86c415370d389e30b9f0a3c02d25d0082e8ad6f3f1ef24a45c3cf82b383367063a4d4613e4264f01b2dac2e5aa42043
f8fb5f69fa871d14fb273e767a531c40f02f343bc2fb45a0c7e0f6be2561923a77211d66a6e2dbb43c366350beae22da3a
c2c1f5077096fcb5c4bf255f7574351ae0b1e1f03632817c0856d4a8ba97afbdc8b85855402bc56926fcec209f9ea8":"70
f382bddf4d5d2dd88b3bc7b7308be632b84045":"84ebeb481be59845b46468bafb471c0112e02b235d84b5d911cbd19
26ee5074ae0424495cb20e82308b8ebb65f419a03fb40e72b78981d88aad143053685172c97b29c8b7bf0ae73b5b2263
c403da0ed2f80ff7450af7828eb8b86f0028bd2a8b176a4d228cccea18394f238b09ff758cc00bc04301152355742f282b
54e663a919e709d8da24ade5500a7b9aa50226e0ca52923e6c2d860ec50ff480fa57477e82b0565f4379f79c772d5c2da
80af9fbf325ece6fc20b00961614bee89a183e":0

RSASSA-PSS

Signature Example 9_4 (verify)

pkcs1_rsassa_pss_verify:1536:16:"e6bd692ac96645790403fdd0f5beb8b9bf92ed10007fc365046419dd06c05c5b5b2
f48ecf989e4ce269109979cbb40b4a0ad24d22483d1ee315ad4ccb1534268352691c524f6dd8e6c29d224cf246973aec8
6c5bf6b1401a850d1b9ad1bb8cbcec47b06f0f8c7f45d3fc8f319299c5433ddbc2b3053b47ded2ecd4a4caefd614833dc8
bb622f317ed076b8057fe8de3f84480ad5e83e4a61904a4f248fb397027357e1d30e463139815c6fd4fd5ac5b8172a452
30ecb6318a04f1455d84e5a8b":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"1dfd43b46c93db82
629bdae2bd0a12b882ea04c3b465f5cf93023f01059626dbbe99f26bb1be949dddd16dc7f3debb19a194627f0b224434
df7d8700e9e98b06e360c12fdbe3d19f51c9684eb9089ecbb0a2f0450399d3f59eac7294085d044f5393c6ce737423d8b
86c415370d389e30b9f0a3c02d25d0082e8ad6f3f1ef24a45c3cf82b383367063a4d4613e4264f01b2dac2e5aa42043f8f
b5f69fa871d14fb273e767a531c40f02f343bc2fb45a0c7e0f6be2561923a77211d66a6e2dbb43c366350beae22da3ac2c
1f5077096fcb5c4bf255f7574351ae0b1e1f03632817c0856d4a8ba97afbdc8b85855402bc56926fcec209f9ea8":"70f38
2bddf4d5d2dd88b3bc7b7308be632b84045":"84ebeb481be59845b46468bafb471c0112e02b235d84b5d911cbd1926e
e5074ae0424495cb20e82308b8ebb65f419a03fb40e72b78981d88aad143053685172c97b29c8b7bf0ae73b5b2263c40
3da0ed2f80ff7450af7828eb8b86f0028bd2a8b176a4d228cccea18394f238b09ff758cc00bc04301152355742f282b54e
663a919e709d8da24ade5500a7b9aa50226e0ca52923e6c2d860ec50ff480fa57477e82b0565f4379f79c772d5c2da80a
f9fbf325ece6fc20b00961614bee89a183e":0

RSASSA-PSS

Signature Example 9_5

pkcs1_rsassa_pss_sign:1536:16:"f8eb97e98df12664eefdb761596a69ddcd0e76daece6ed4bf5a1b50ac086f7928a4d2f8726a77e515b74da41988f220b1cc87aa1fc810ce99a82f2d1ce821edced794c6941f42c7a1a0b8c4d28c75ec60b652279f6154a762aed165d47dee367":16:"ed4d71d0a6e24b93c2e5f6b4bbe05f5fb0afa042d204fe3378d365c2f288b6a8dad7efe45d153eef40cacc7b81ff934002d108994b94a5e4728cd9c963375ae49965bda55cbf0efed8d6553b4027f2d86208a6e6b489c176128092d629e49d3d":16:"e6bd692ac96645790403fdd0f5beb8b9bf92ed10007fc365046419dd06c05c5b5b2f48ecf989e4ce269109979cbb40b4a0ad24d22483d1ee315ad4ccb1534268352691c524f6dd8e6c29d224cf246973aec86c5bf6b1401a850d1b9ad1bb8cbcec47b06f0f8c7f45d3fc8f319299c5433ddbc2b3053b47ded2ecd4a4caefd614833dc8bb622f317ed076b8057fe8de3f84480ad5e83e4a61904a4f248fb397027357e1d30e463139815c6fd4fd5ac5b8172a45230ecb6318a04f1455d84e5a8b":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"1bdc6e7c98fb8cf54e9b097b66a831e9cfe52d9d4888448ee4b0978093ba1d7d73ae78b3a62ba4ad95cd289ccb9e005226bb3d178bccaa821fb044a4e21ee97696c14d0678c94c2dae93b0ad73922218553daa7e44ebe57725a7a45cc72b9b2138a6b17c8db411ce8279ee1241aff0a8bec6f77f87edb0c69cb27236e3435a800b192e4f11e519e3fe30fc30eaccca4fbb41769029bf708e817a9e683805be67fa100984683b74838e3bcffa79366eed1d481c76729118838f31ba8a048a93c1be4424598e8df6328b7a77880a3f9c7e2e8dfca8eb5a26fb86bdc556d42bbe01d9fa6ed80646491c9341":"d689257a86effa68212c5e0c619eca295fb91b67":"82102df8cb91e7179919a04d26d335d64fbc2f872c44833943241de8454810274cdf3db5f42d423db152af7135f701420e39b494a67cbfd19f9119da233a23da5c6439b5ba0d2bc373eee3507001378d4a4073856b7fe2aba0b5ee93b27f4afec7d4d120921c83f606765b02c19e4d6a1a3b95fa4c422951be4f52131077ef17179729cddfbdb56950dbaceefe78cb16640a099ea56d24389eef10f8fecb31ba3ea3b227c0a86698bb89e3e9363905bf22777b2a3aa521b65b4cef76d83bde4c":0

RSASSA-PSS

Signature Example 9_5 (verify)

pkcs1_rsassa_pss_verify:1536:16:"e6bd692ac96645790403fdd0f5beb8b9bf92ed10007fc365046419dd06c05c5b5b2f48ecf989e4ce269109979cbb40b4a0ad24d22483d1ee315ad4ccb1534268352691c524f6dd8e6c29d224cf246973aec86c5bf6b1401a850d1b9ad1bb8cbcec47b06f0f8c7f45d3fc8f319299c5433ddbc2b3053b47ded2ecd4a4caefd614833dc8bb622f317ed076b8057fe8de3f84480ad5e83e4a61904a4f248fb397027357e1d30e463139815c6fd4fd5ac5b8172a45230ecb6318a04f1455d84e5a8b":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"1bdc6e7c98fb8cf54e9b097b66a831e9cfe52d9d4888448ee4b0978093ba1d7d73ae78b3a62ba4ad95cd289ccb9e005226bb3d178bccaa821fb044a4e21ee97696c14d0678c94c2dae93b0ad73922218553daa7e44ebe57725a7a45cc72b9b2138a6b17c8db411ce8279ee1241aff0a8bec6f77f87edb0c69cb27236e3435a800b192e4f11e519e3fe30fc30eaccca4fbb41769029bf708e817a9e683805be67fa100984683b74838e3bcffa79366eed1d481c76729118838f31ba8a048a93c1be4424598e8df6328b7a77880a3f9c7e2e8dfca8eb5a26fb86bdc556d42bbe01d9fa6ed80646491c9341":"d689257a86effa68212c5e0c619eca295fb91b67":"82102df8cb91e7179919a04d26d335d64fbc2f872c44833943241de8454810274cdf3db5f42d423db152af7135f701420e39b494a67cbfd19f9119da233a23da5c6439b5ba0d2bc373eee3507001378d4a4073856b7fe2aba0b5ee93b27f4afec7d4d120921c83f606765b02c19e4d6a1a3b95fa4c422951be4f52131077ef17179729cddfbdb56950dbaceefe78cb16640a099ea56d24389eef10f8fecb31ba3ea3b227c0a86698bb89e3e9363905bf22777b2a3aa521b65b4cef76d83bde4c":0

RSASSA-PSS

Signature Example 9_6

pkcs1_rsassa_pss_sign:1536:16:"f8eb97e98df12664eefdb761596a69ddcd0e76daece6ed4bf5a1b50ac086f7928a4d2f8726a77e515b74da41988f220b1cc87aa1fc810ce99a82f2d1ce821edced794c6941f42c7a1a0b8c4d28c75ec60b652279f6154a762aed165d47dee367":16:"ed4d71d0a6e24b93c2e5f6b4bbe05f5fb0afa042d204fe3378d365c2f288b6a8dad7efe45d153eef40cacc7b81ff934002d108994b94a5e4728cd9c963375ae49965bda55cbf0efed8d6553b4027f2d86208a6e6b489c176128092d629e49d3d":16:"e6bd692ac96645790403fdd0f5beb8b9bf92ed10007fc365046419dd06c05c5b5

b2f48ecf989e4ce269109979cbb40b4a0ad24d22483d1ee315ad4ccb1534268352691c524f6dd8e6c29d224cf246973ae
c86c5bf6b1401a850d1b9ad1bb8cbcec47b06f0f8c7f45d3fc8f319299c5433ddbc2b3053b47ded2ecd4a4caefd614833d
c8bb622f317ed076b8057fe8de3f84480ad5e83e4a61904a4f248fb397027357e1d30e463139815c6fd4fd5ac5b8172a4
5230ecb6318a04f1455d84e5a8b":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"88c7a9f1360401
d90e53b101b61c5325c3c75db1b411fbeb8e830b75e96b56670ad245404e16793544ee354bc613a90cc9848715a73db
5893e7f6d279815c0c1de83ef8e2956e3a56ed26a888d7a9cdcd042f4b16b7fa51ef1a0573662d16a302d0ec5b285d2e0
3ad96529c87b3d374db372d95b2443d061b6b1a350ba87807ed083afd1eb05c3f52f4eba5ed2227714fdb50b9d9d9dd6
814f62f6272fcd5cdbce7a9ef797":"c25f13bf67d081671a0481a1f1820d613bba2276":"a7fdb0d259165ca2c88d00bbf
1028a867d337699d061193b17a9648e14ccbbaadeacaacdec815e7571294ebb8a117af205fa078b47b0712c199e3ad05
135c504c24b81705115740802487992ffd511d4afc6b854491eb3f0dd523139542ff15c3101ee85543517c6a3c79417c
67e2dd9aa741e9a29b06dcb593c2336b3670ae3afbac7c3e76e215473e866e338ca244de00b62624d6b9426822ceae9f
8cc460895f41250073fd45c5a1e7b425c204a423a699159f6903e710b37a7bb2bc8049f":0

RSASSA-PSS

Signature Example 9_6 (verify)

pkcs1_rsassa_pss_verify:1536:16:"e6bd692ac96645790403fdd0f5beb8b9bf92ed10007fc365046419dd06c05c5b5b2
f48ecf989e4ce269109979cbb40b4a0ad24d22483d1ee315ad4ccb1534268352691c524f6dd8e6c29d224cf246973aec8
6c5bf6b1401a850d1b9ad1bb8cbcec47b06f0f8c7f45d3fc8f319299c5433ddbc2b3053b47ded2ecd4a4caefd614833dc8
bb622f317ed076b8057fe8de3f84480ad5e83e4a61904a4f248fb397027357e1d30e463139815c6fd4fd5ac5b8172a452
30ecb6318a04f1455d84e5a8b":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"88c7a9f1360401d9
0e53b101b61c5325c3c75db1b411fbeb8e830b75e96b56670ad245404e16793544ee354bc613a90cc9848715a73db58
93e7f6d279815c0c1de83ef8e2956e3a56ed26a888d7a9cdcd042f4b16b7fa51ef1a0573662d16a302d0ec5b285d2e03a
d96529c87b3d374db372d95b2443d061b6b1a350ba87807ed083afd1eb05c3f52f4eba5ed2227714fdb50b9d9d9dd681
4f62f6272fcd5cdbce7a9ef797":"c25f13bf67d081671a0481a1f1820d613bba2276":"a7fdb0d259165ca2c88d00bbf10
28a867d337699d061193b17a9648e14ccbbaadeacaacdec815e7571294ebb8a117af205fa078b47b0712c199e3ad0513
5c504c24b81705115740802487992ffd511d4afc6b854491eb3f0dd523139542ff15c3101ee85543517c6a3c79417c67e
2dd9aa741e9a29b06dcb593c2336b3670ae3afbac7c3e76e215473e866e338ca244de00b62624d6b9426822ceae9f8cc4
60895f41250073fd45c5a1e7b425c204a423a699159f6903e710b37a7bb2bc8049f":0

RSASSA-PSS

Signature Example 10_1

pkcs1_rsassa_pss_sign:2048:16:"cfd50283feeeb97f6f08d73cbc7b3836f82bbcd499479f5e6f76fdfcb8b38c4f71dc9e8
8bd6a6f76371afd65d2af1862b32afb34a95f71b8b132043ffebe3a952baf7592448148c03f9c69b1d68e4ce5cf32c86baf
46fed301ca1ab403069b32f456b91f71898ab081cd8c4252ef5271915c9794b8f295851da7510f99cb73eb":16:"cc4e90
d2a1b3a065d3b2d1f5a8fce31b544475664eab561d2971b99fb7bef844e8ec1f360b8c2ac8359692971ea6a38f723fcc21
1f5dbcb177a0fdac5164a1d4ff7fbb4e829986353cb983659a148cdd420c7d31ba3822ea90a32be46c030e8c17e1fa0ad
37859e06b0aa6fa3b216d9cbe6c0e22339769c0a615913e5da719cf":16:"a5dd867ac4cb02f90b9457d48c14a770ef991
c56c39c0ec65fd11afa8937cea57b9be7ac73b45c0017615b82d622e318753b6027c0fd157be12f8090fee2a7adcd0eef7
59f88ba4997c7a42d58c9aa12cb99ae001fe521c13bb5431445a8d5ae4f5e4c7e948ac227d3604071f20e577e905fbeb1
5dfaf06d1de5ae6253d63a6a2120b31a5da5dabc9550600e20f27d3739e2627925fea3cc509f21dff04e6eea4549c540d6
809ff9307eede91fff58733d8385a237d6d3705a33e391900992070df7adf1357cf7e3700ce3667de83f17b8df1778db38
1dce09cb4ad058a511001a738198ee27cf55a13b754539906582ec8b174bd58d5d1f3d767c613721ae05":16:"010001"
:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"883177e5126b9be2d9a9680327d5370c6f26861f5820c43da67a3
ad609":"04e215ee6ff934b9da70d7730c8734abfcecde89":"82c2b160093b8aa3c0f7522b19f87354066c77847abf2a9f
ce542d0e84e920c5afb49ffdfdace16560ee94a1369601148ebad7a0e151cf16331791a5727d05f21e74e7eb811440206
935d744765a15e79f015cb66c532c87a6a05961c8bfad741a9a6657022894393e7223739796c02a77455d0f555b0ec01
ddf259b6207fd0fd57614cef1a5573baaff4ec00069951659b85f24300a25160ca8522dc6e6727e57d019d7e63629b8fe
5e89e25cc15beb3a647577559299280b9b28f79b0409000be25bbd96408ba3b43cc486184dd1c8e62553fa1af4040f60

663de7f5e49c04388e257f1ce89c95dab48a315d9b66b1b7628233876ff2385230d070d07e1666":0

RSASSA-PSS
Signature Example 10_1 (verify)
pkcs1_rsassa_pss_verify:2048:16:"a5dd867ac4cb02f90b9457d48c14a770ef991c56c39c0ec65fd11afa8937cea57b9b
e7ac73b45c0017615b82d622e318753b6027c0fd157be12f8090fee2a7adcd0eef759f88ba4997c7a42d58c9aa12cb99a
e001fe521c13bb5431445a8d5ae4f5e4c7e948ac227d3604071f20e577e905fbeb15dfaf06d1de5ae6253d63a6a2120b3
1a5da5dabc9550600e20f27d3739e2627925fea3cc509f21dff04e6eea4549c540d6809ff9307eede91fff58733d8385a23
7d6d3705a33e391900992070df7adf1357cf7e3700ce3667de83f17b8df1778db381dce09cb4ad058a511001a738198ee
27cf55a13b754539906582ec8b174bd58d5d1f3d767c613721ae05":16:"010001":MBEDTLS_MD_SHA1:MBEDTL
S_MD_SHA1:"883177e5126b9be2d9a9680327d5370c6f26861f5820c43da67a3ad609":"04e215ee6ff934b9da70d77
30c8734abfcecde89":"82c2b160093b8aa3c0f7522b19f87354066c77847abf2a9fce542d0e84e920c5afb49ffdfdace16
560ee94a1369601148ebad7a0e151cf16331791a5727d05f21e74e7eb811440206935d744765a15e79f015cb66c532c8
7a6a05961c8bfad741a9a6657022894393e7223739796c02a77455d0f555b0ec01ddf259b6207fd0fd57614cef1a5573b
aaff4ec00069951659b85f24300a25160ca8522dc6e6727e57d019d7e63629b8fe5e89e25cc15beb3a64757755929928
0b9b28f79b0409000be25bbd96408ba3b43cc486184dd1c8e62553fa1af4040f60663de7f5e49c04388e257f1ce89c95d
ab48a315d9b66b1b7628233876ff2385230d070d07e1666":0

RSASSA-PSS
Signature Example 10_2
pkcs1_rsassa_pss_sign:2048:16:"cfd50283feeeb97f6f08d73cbc7b3836f82bbcd499479f5e6f76fdfcb8b38c4f71dc9e8
8bd6a6f76371afd65d2af1862b32afb34a95f71b8b132043ffebe3a952baf7592448148c03f9c69b1d68e4ce5cf32c86baf
46fed301ca1ab403069b32f456b91f71898ab081cd8c4252ef5271915c9794b8f295851da7510f99cb73eb":16:"cc4e90
d2a1b3a065d3b2d1f5a8fce31b544475664eab561d2971b99fb7bef844e8ec1f360b8c2ac8359692971ea6a38f723fcc21
1f5dbcb177a0fdac5164a1d4ff7fbb4e829986353cb983659a148cdd420c7d31ba3822ea90a32be46c030e8c17e1fa0ad
37859e06b0aa6fa3b216d9cbe6c0e22339769c0a615913e5da719cf":16:"a5dd867ac4cb02f90b9457d48c14a770ef991
c56c39c0ec65fd11afa8937cea57b9be7ac73b45c0017615b82d622e318753b6027c0fd157be12f8090fee2a7adcd0eef7
59f88ba4997c7a42d58c9aa12cb99ae001fe521c13bb5431445a8d5ae4f5e4c7e948ac227d3604071f20e577e905fbeb1
5dfaf06d1de5ae6253d63a6a2120b31a5da5dabc9550600e20f27d3739e2627925fea3cc509f21dff04e6eea4549c540d6
809ff9307eede91fff58733d8385a237d6d3705a33e391900992070df7adf1357cf7e3700ce3667de83f17b8df1778db38
1dce09cb4ad058a511001a738198ee27cf55a13b754539906582ec8b174bd58d5d1f3d767c613721ae05":16:"010001"
:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"dd670a01465868adc93f26131957a50c52fb777cdbaa30892c9e1
2361164ec13979d43048118e4445db87bee58dd987b3425d02071d8dbae80708b039dbb64dbd1de5657d9fed0c118a5
4143742e0ff3c87f74e45857647af3f79eb0a14c9d75ea9a1a04b7cf478a897a708fd988f48e801edb0b7039df8c23bb3c
56f4e821ac":"8b2bdd4b40faf545c778ddf9bc1a49cb57f9b71b":"14ae35d9dd06ba92f7f3b897978aed7cd4bf5ff0b585
a40bd46ce1b42cd2703053bb9044d64e813d8f96db2dd7007d10118f6f8f8496097ad75e1ff692341b2892ad55a633a1
c55e7f0a0ad59a0e203a5b8278aec54dd8622e2831d87174f8caff43ee6c46445345d84a59659bfb92ecd4c818668695f
34706f66828a89959637f2bf3e3251c24bdba4d4b7649da0022218b119c84e79a6527ec5b8a5f861c159952e23ec05e1
e717346faefe8b1686825bd2b262fb2531066c0de09acde2e4231690728b5d85e115a2f6b92b79c25abc9bd9399ff8bcf
825a52ea1f56ea76dd26f43baafa18bfa92a504cbd35699e26d1dcc5a2887385f3c63232f06f3244c3":0

RSASSA-PSS
Signature Example 10_2 (verify)
pkcs1_rsassa_pss_verify:2048:16:"a5dd867ac4cb02f90b9457d48c14a770ef991c56c39c0ec65fd11afa8937cea57b9b
e7ac73b45c0017615b82d622e318753b6027c0fd157be12f8090fee2a7adcd0eef759f88ba4997c7a42d58c9aa12cb99a
e001fe521c13bb5431445a8d5ae4f5e4c7e948ac227d3604071f20e577e905fbeb15dfaf06d1de5ae6253d63a6a2120b3
1a5da5dabc9550600e20f27d3739e2627925fea3cc509f21dff04e6eea4549c540d6809ff9307eede91fff58733d8385a23
7d6d3705a33e391900992070df7adf1357cf7e3700ce3667de83f17b8df1778db381dce09cb4ad058a511001a738198ee

27cf55a13b754539906582ec8b174bd58d5d1f3d767c613721ae05":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"dd670a01465868adc93f26131957a50c52fb777cdbaa30892c9e12361164ec13979d43048118e4445db87bee58dd987b3425d02071d8dbae80708b039dbb64dbd1de5657d9fed0c118a54143742e0ff3c87f74e45857647af3f79eb0a14c9d75ea9a1a04b7cf478a897a708fd988f48e801edb0b7039df8c23bb3c56f4e821ac":"8b2bdd4b40faf545c778ddf9bc1a49cb57f9b71b":"14ae35d9dd06ba92f7f3b897978aed7cd4bf5ff0b585a40bd46ce1b42cd2703053bb9044d64e813d8f96db2dd7007d10118f6f8f8496097ad75e1ff692341b2892ad55a633a1c55e7f0a0ad59a0e203a5b8278aec54dd8622e2831d87174f8caff43ee6c46445345d84a59659bfb92ecd4c818668695f34706f66828a89959637f2bf3e3251c24bdba4d4b7649da0022218b119c84e79a6527ec5b8a5f861c159952e23ec05e1e717346faefe8b1686825bd2b262fb2531066c0de09acde2e4231690728b5d85e115a2f6b92b79c25abc9bd9399ff8bcf825a52ea1f56ea76dd26f43baafa18bfa92a504cbd35699e26d1dcc5a2887385f3c63232f06f3244c3":0

RSASSA-PSS

Signature Example 10_3

pkcs1_rsassa_pss_sign:2048:16:"cfd50283feeeb97f6f08d73cbc7b3836f82bbcd499479f5e6f76fdfcb8b38c4f71dc9e88bd6a6f76371afd65d2af1862b32afb34a95f71b8b132043ffebe3a952baf7592448148c03f9c69b1d68e4ce5cf32c86baf46fed301ca1ab403069b32f456b91f71898ab081cd8c4252ef5271915c9794b8f295851da7510f99cb73eb":16:"cc4e90d2a1b3a065d3b2d1f5a8fce31b544475664eab561d2971b99fb7bef844e8ec1f360b8c2ac8359692971ea6a38f723fcc211f5dbcb177a0fdac5164a1d4ff7fbb4e829986353cb983659a148cdd420c7d31ba3822ea90a32be46c030e8c17e1fa0ad37859e06b0aa6fa3b216d9cbe6c0e22339769c0a615913e5da719cf":16:"a5dd867ac4cb02f90b9457d48c14a770ef991c56c39c0ec65fd11afa8937cea57b9be7ac73b45c0017615b82d622e318753b6027c0fd157be12f8090fee2a7adcd0eef759f88ba4997c7a42d58c9aa12cb99ae001fe521c13bb5431445a8d5ae4f5e4c7e948ac227d3604071f20e577e905fbeb15dfaf06d1de5ae6253d63a6a2120b31a5da5dabc9550600e20f27d3739e2627925fea3cc509f21dff04e6eea4549c540d6809ff9307eede91fff58733d8385a237d6d3705a33e391900992070df7adf1357cf7e3700ce3667de83f17b8df1778db381dce09cb4ad058a511001a738198ee27cf55a13b754539906582ec8b174bd58d5d1f3d767c613721ae05":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"48b2b6a57a63c84cea859d65c668284b08d96bdcaabe252db0e4a96cb1bac6019341db6fbefb8d106b0e90eda6bcc6c6262f37e7ea9c7e5d226bd7df85ec5e71efff2f54c5db577ff729ff91b842491de2741d0c631607df586b905b23b91af13da12304bf83eca8a73e871ff9db":"4e96fc1b398f92b44671010c0dc3efd6e20c2d73":"6e3e4d7b6b15d2fb46013b8900aa5bbb3939cf2c095717987042026ee62c74c54cffd5d7d57efbbf950a0f5c574fa09d3fc1c9f513b05b4ff50dd8df7edfa20102854c35e592180119a70ce5b085182aa02d9ea2aa90d1df03f2daae885ba2f5d05afdac97476f06b93b5bc94a1a80aa9116c4d615f333b098892b25fface266f5db5a5a3bcc10a824ed55aad35b727834fb8c07da28fcf416a5d9b2224f1f8b442b36f91e456fdea2d7cfe3367268de0307a4c74e924159ed33393d5e0655531c77327b89821bdedf880161c78cd4196b5419f7acc3f13e5ebf161b6e7c6724716ca33b85c2e25640192ac2859651d50bde7eb976e51cec828b98b6563b86bb":0

RSASSA-PSS

Signature Example 10_3 (verify)

pkcs1_rsassa_pss_verify:2048:16:"a5dd867ac4cb02f90b9457d48c14a770ef991c56c39c0ec65fd11afa8937cea57b9be7ac73b45c0017615b82d622e318753b6027c0fd157be12f8090fee2a7adcd0eef759f88ba4997c7a42d58c9aa12cb99ae001fe521c13bb5431445a8d5ae4f5e4c7e948ac227d3604071f20e577e905fbeb15dfaf06d1de5ae6253d63a6a2120b31a5da5dabc9550600e20f27d3739e2627925fea3cc509f21dff04e6eea4549c540d6809ff9307eede91fff58733d8385a237d6d3705a33e391900992070df7adf1357cf7e3700ce3667de83f17b8df1778db381dce09cb4ad058a511001a738198ee27cf55a13b754539906582ec8b174bd58d5d1f3d767c613721ae05":16:"010001":MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"48b2b6a57a63c84cea859d65c668284b08d96bdcaabe252db0e4a96cb1bac6019341db6fbefb8d106b0e90eda6bcc6c6262f37e7ea9c7e5d226bd7df85ec5e71efff2f54c5db577ff729ff91b842491de2741d0c631607df586b905b23b91af13da12304bf83eca8a73e871ff9db":"4e96fc1b398f92b44671010c0dc3efd6e20c2d73":"6e3e4d7b6b15d2fb46013b8900aa5bbb3939cf2c095717987042026ee62c74c54cffd5d7d57efbbf950a0f5c574fa09d3fc1c9f513b05b4ff50dd8df7edfa20102854c35e592180119a70ce5b085182aa02d9ea2aa90d1df03f2daae885ba2f5d05afdac97476f06b93b5bc94a1a80aa9116c4d615f333b098892b25fface266f5db5a5a3bcc10a824ed55aad35b727834fb8c07da28fcf416a5d

9b2224f1f8b442b36f91e456fdea2d7cfe3367268de0307a4c74e924159ed33393d5e0655531c77327b89821bdedf8801
61c78cd4196b5419f7acc3f13e5ebf161b6e7c6724716ca33b85c2e25640192ac2859651d50bde7eb976e51cec828b98
b6563b86bb":0

RSASSA-PSS
Signature Example 10_4
pkcs1_rsassa_pss_sign:2048:16:"cfd50283feeeb97f6f08d73cbc7b3836f82bbcd499479f5e6f76fdfcb8b38c4f71dc9e8
8bd6a6f76371afd65d2af1862b32afb34a95f71b8b132043ffebe3a952baf7592448148c03f9c69b1d68e4ce5cf32c86baf
46fed301ca1ab403069b32f456b91f71898ab081cd8c4252ef5271915c9794b8f295851da7510f99cb73eb":16:"cc4e90
d2a1b3a065d3b2d1f5a8fce31b544475664eab561d2971b99fb7bef844e8ec1f360b8c2ac8359692971ea6a38f723fcc21
1f5dbcb177a0fdac5164a1d4ff7fbb4e829986353cb983659a148cdd420c7d31ba3822ea90a32be46c030e8c17e1fa0ad
37859e06b0aa6fa3b216d9cbe6c0e22339769c0a615913e5da719cf":16:"a5dd867ac4cb02f90b9457d48c14a770ef991
c56c39c0ec65fd11afa8937cea57b9be7ac73b45c0017615b82d622e318753b6027c0fd157be12f8090fee2a7adcd0eef7
59f88ba4997c7a42d58c9aa12cb99ae001fe521c13bb5431445a8d5ae4f5e4c7e948ac227d3604071f20e577e905fbeb1
5dfaf06d1de5ae6253d63a6a2120b31a5da5dabc9550600e20f27d3739e2627925fea3cc509f21dff04e6eea4549c540d6
809ff9307eede91fff58733d8385a237d6d3705a33e391900992070df7adf1357cf7e3700ce3667de83f17b8df1778db38
1dce09cb4ad058a511001a738198ee27cf55a13b754539906582ec8b174bd58d5d1f3d767c613721ae05":16:"010001"
:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"0b8777c7f839baf0a64bbbdbc5ce79755c57a205b845c174e2d2e
90546a089c4e6ec8adffa23a7ea97bae6b65d782b82db5d2b5a56d22a29a05e7c4433e2b82a621abba90add05ce393fc4
8a840542451a":"c7cd698d84b65128d8835e3a8b1eb0e01cb541ec":"34047ff96c4dc0dc90b2d4ff59a1a361a4754b25
5d2ee0af7d8bf87c9bc9e7ddeede33934c63ca1c0e3d262cb145ef932a1f2c0a997aa6a34f8eaee7477d82ccf09095a6b8
acad38d4eec9fb7eab7ad02da1d11d8e54c1825e55bf58c2a23234b902be124f9e9038a8f68fa45dab72f66e0945bf1d8b
acc9044c6f07098c9fcec58a3aab100c805178155f030a124c450e5acbda47d0e4f10b80a23f803e774d023b0015c20b9f
9bbe7c91296338d5ecb471cafb032007b67a60be5f69504a9f01abb3cb467b260e2bce860be8d95bf92c0c8e1496ed1e5
28593a4abb6df462dde8a0968dffe4683116857a232f5ebf6c85be238745ad0f38f767a5fdbf486fb":0

RSASSA-PSS
Signature Example 10_4 (verify)
pkcs1_rsassa_pss_verify:2048:16:"a5dd867ac4cb02f90b9457d48c14a770ef991c56c39c0ec65fd11afa8937cea57b9b
e7ac73b45c0017615b82d622e318753b6027c0fd157be12f8090fee2a7adcd0eef759f88ba4997c7a42d58c9aa12cb99a
e001fe521c13bb5431445a8d5ae4f5e4c7e948ac227d3604071f20e577e905fbeb15dfaf06d1de5ae6253d63a6a2120b3
1a5da5dabc9550600e20f27d3739e2627925fea3cc509f21dff04e6eea4549c540d6809ff9307eede91fff58733d8385a23
7d6d3705a33e391900992070df7adf1357cf7e3700ce3667de83f17b8df1778db381dce09cb4ad058a511001a738198ee
27cf55a13b754539906582ec8b174bd58d5d1f3d767c613721ae05":16:"010001":MBEDTLS_MD_SHA1:MBEDTL
S_MD_SHA1:"0b8777c7f839baf0a64bbbdbc5ce79755c57a205b845c174e2d2e90546a089c4e6ec8adffa23a7ea97ba
e6b65d782b82db5d2b5a56d22a29a05e7c4433e2b82a621abba90add05ce393fc48a840542451a":"c7cd698d84b6512
8d8835e3a8b1eb0e01cb541ec":"34047ff96c4dc0dc90b2d4ff59a1a361a4754b255d2ee0af7d8bf87c9bc9e7ddeede33
934c63ca1c0e3d262cb145ef932a1f2c0a997aa6a34f8eaee7477d82ccf09095a6b8acad38d4eec9fb7eab7ad02da1d11d
8e54c1825e55bf58c2a23234b902be124f9e9038a8f68fa45dab72f66e0945bf1d8bacc9044c6f07098c9fcec58a3aab10
0c805178155f030a124c450e5acbda47d0e4f10b80a23f803e774d023b0015c20b9f9bbe7c91296338d5ecb471cafb032
007b67a60be5f69504a9f01abb3cb467b260e2bce860be8d95bf92c0c8e1496ed1e528593a4abb6df462dde8a0968dffe
4683116857a232f5ebf6c85be238745ad0f38f767a5fdbf486fb":0

RSASSA-PSS
Signature Example 10_5
pkcs1_rsassa_pss_sign:2048:16:"cfd50283feeeb97f6f08d73cbc7b3836f82bbcd499479f5e6f76fdfcb8b38c4f71dc9e8
8bd6a6f76371afd65d2af1862b32afb34a95f71b8b132043ffebe3a952baf7592448148c03f9c69b1d68e4ce5cf32c86baf
46fed301ca1ab403069b32f456b91f71898ab081cd8c4252ef5271915c9794b8f295851da7510f99cb73eb":16:"cc4e90

d2a1b3a065d3b2d1f5a8fce31b544475664eab561d2971b99fb7bef844e8ec1f360b8c2ac8359692971ea6a38f723fcc21
1f5dbcb177a0fdac5164a1d4ff7fbb4e829986353cb983659a148cdd420c7d31ba3822ea90a32be46c030e8c17e1fa0ad
37859e06b0aa6fa3b216d9cbe6c0e22339769c0a615913e5da719cf":16:"a5dd867ac4cb02f90b9457d48c14a770ef991
c56c39c0ec65fd11afa8937cea57b9be7ac73b45c0017615b82d622e318753b6027c0fd157be12f8090fee2a7adcd0eef7
59f88ba4997c7a42d58c9aa12cb99ae001fe521c13bb5431445a8d5ae4f5e4c7e948ac227d3604071f20e577e905fbeb1
5dfaf06d1de5ae6253d63a6a2120b31a5da5dabc9550600e20f27d3739e2627925fea3cc509f21dff04e6eea4549c540d6
809ff9307eede91fff58733d8385a237d6d3705a33e391900992070df7adf1357cf7e3700ce3667de83f17b8df1778db38
1dce09cb4ad058a511001a738198ee27cf55a13b754539906582ec8b174bd58d5d1f3d767c613721ae05":16:"010001"
:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"f1036e008e71e964dadc9219ed30e17f06b4b68a955c16b312b1e
ddf028b74976bed6b3f6a63d4e77859243c9cccdc98016523abb02483b35591c33aad81213bb7c7bb1a470aabc10d442
56c4d4559d916":"efa8bff96212b2f4a3f371a10d574152655f5dfb":"7e0935ea18f4d6c1d17ce82eb2b3836c55b38458
9ce19dfe743363ac9948d1f346b7bfddfe92efd78adb21faefc89ade42b10f374003fe122e67429a1cb8cbd1f8d9014564c
44d120116f4990f1a6e38774c194bd1b8213286b077b0499d2e7b3f434ab12289c556684deed78131934bb3dd653723
6f7c6f3dcb09d476be07721e37e1ceed9b2f7b406887bd53157305e1c8b4f84d733bc1e186fe06cc59b6edb8f4bd7ffefd
f4f7ba9cfb9d570689b5a1a4109a746a690893db3799255a0cb9215d2d1cd490590e952e8c8786aa0011265252470c04
1dfbc3eec7c3cbf71c24869d115c0cb4a956f56d530b80ab589acfefc690751ddf36e8d383f83cedd2cc":0

RSASSA-PSS

Signature Example 10_5 (verify)

pkcs1_rsassa_pss_verify:2048:16:"a5dd867ac4cb02f90b9457d48c14a770ef991c56c39c0ec65fd11afa8937cea57b9b
e7ac73b45c0017615b82d622e318753b6027c0fd157be12f8090fee2a7adcd0eef759f88ba4997c7a42d58c9aa12cb99a
e001fe521c13bb5431445a8d5ae4f5e4c7e948ac227d3604071f20e577e905fbeb15dfaf06d1de5ae6253d63a6a2120b3
1a5da5dabc9550600e20f27d3739e2627925fea3cc509f21dff04e6eea4549c540d6809ff9307eede91fff58733d8385a23
7d6d3705a33e391900992070df7adf1357cf7e3700ce3667de83f17b8df1778db381dce09cb4ad058a511001a738198ee
27cf55a13b754539906582ec8b174bd58d5d1f3d767c613721ae05":16:"010001":MBEDTLS_MD_SHA1:MBEDTL
S_MD_SHA1:"f1036e008e71e964dadc9219ed30e17f06b4b68a955c16b312b1eddf028b74976bed6b3f6a63d4e7785
9243c9cccdc98016523abb02483b35591c33aad81213bb7c7bb1a470aabc10d44256c4d4559d916":"efa8bff96212b2f
4a3f371a10d574152655f5dfb":"7e0935ea18f4d6c1d17ce82eb2b3836c55b384589ce19dfe743363ac9948d1f346b7bf
ddfe92efd78adb21faefc89ade42b10f374003fe122e67429a1cb8cbd1f8d9014564c44d120116f4990f1a6e38774c194b
d1b8213286b077b0499d2e7b3f434ab12289c556684deed78131934bb3dd6537236f7c6f3dcb09d476be07721e37e1c
eed9b2f7b406887bd53157305e1c8b4f84d733bc1e186fe06cc59b6edb8f4bd7ffefdf4f7ba9cfb9d570689b5a1a4109a7
46a690893db3799255a0cb9215d2d1cd490590e952e8c8786aa0011265252470c041dfbc3eec7c3cbf71c24869d115c0
cb4a956f56d530b80ab589acfefc690751ddf36e8d383f83cedd2cc":0

RSASSA-PSS

Signature Example 10_6

pkcs1_rsassa_pss_sign:2048:16:"cfd50283feeeb97f6f08d73cbc7b3836f82bbcd499479f5e6f76fdfcb8b38c4f71dc9e8
8bd6a6f76371afd65d2af1862b32afb34a95f71b8b132043ffebe3a952baf7592448148c03f9c69b1d68e4ce5cf32c86baf
46fed301ca1ab403069b32f456b91f71898ab081cd8c4252ef5271915c9794b8f295851da7510f99cb73eb":16:"cc4e90
d2a1b3a065d3b2d1f5a8fce31b544475664eab561d2971b99fb7bef844e8ec1f360b8c2ac8359692971ea6a38f723fcc21
1f5dbcb177a0fdac5164a1d4ff7fbb4e829986353cb983659a148cdd420c7d31ba3822ea90a32be46c030e8c17e1fa0ad
37859e06b0aa6fa3b216d9cbe6c0e22339769c0a615913e5da719cf":16:"a5dd867ac4cb02f90b9457d48c14a770ef991
c56c39c0ec65fd11afa8937cea57b9be7ac73b45c0017615b82d622e318753b6027c0fd157be12f8090fee2a7adcd0eef7
59f88ba4997c7a42d58c9aa12cb99ae001fe521c13bb5431445a8d5ae4f5e4c7e948ac227d3604071f20e577e905fbeb1
5dfaf06d1de5ae6253d63a6a2120b31a5da5dabc9550600e20f27d3739e2627925fea3cc509f21dff04e6eea4549c540d6
809ff9307eede91fff58733d8385a237d6d3705a33e391900992070df7adf1357cf7e3700ce3667de83f17b8df1778db38
1dce09cb4ad058a511001a738198ee27cf55a13b754539906582ec8b174bd58d5d1f3d767c613721ae05":16:"010001"
:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:"25f10895a87716c137450bb9519dfaa1f207faa942ea88abf71e9c

17980085b555aebab76264ae2a3ab93c2d12981191ddac6fb5949eb36aee3c5da940f00752c916d94608fa7d97ba6a29
15b688f20323d4e9d96801d89a72ab5892dc2117c07434fcf972e058cf8c41ca4b4ff554f7d5068ad3155fced0f3125bc0
4f9193378a8f5c4c3b8cb4dd6d1cc69d30ecca6eaa51e36a05730e9e342e855baf099defb8afd7":"ad8b1523703646224
b660b550885917ca2d1df28":"6d3b5b87f67ea657af21f75441977d2180f91b2c5f692de82955696a686730d9b9778d9
70758ccb26071c2209ffbd6125be2e96ea81b67cb9b9308239fda17f7b2b64ecda096b6b935640a5a1cb42a9155b1c9ef
7a633a02c59f0d6ee59b852c43b35029e73c940ff0410e8f114eed46bbd0fae165e42be2528a401c3b28fd818ef3232dca
9f4d2a0f5166ec59c42396d6c11dbc1215a56fa17169db9575343ef34f9de32a49cdc3174922f229c23e18e45df935311
9ec4319cedce7a17c64088c1f6f52be29634100b3919d38f3d1ed94e6891e66a73b8fb849f5874df59459e298c7bbce2e
ee782a195aa66fe2d0732b25e595f57d3e061b1fc3e4063bf98f":0

RSASSA-PSS
Signature Example 10_6 (verify)
pkcs1_rsassa_pss_verify:2048:16:"a5dd867ac4cb02f90b9457d48c14a770ef991c56c39c0ec65fd11afa8937cea57b9b
e7ac73b45c0017615b82d622e318753b6027c0fd157be12f8090fee2a7adcd0eef759f88ba4997c7a42d58c9aa12cb99a
e001fe521c13bb5431445a8d5ae4f5e4c7e948ac227d3604071f20e577e905fbeb15dfaf06d1de5ae6253d63a6a2120b3
1a5da5dabc9550600e20f27d3739e2627925fea3cc509f21dff04e6eea4549c540d6809ff9307eede91fff58733d8385a23
7d6d3705a33e391900992070df7adf1357cf7e3700ce3667de83f17b8df1778db381dce09cb4ad058a511001a738198ee
27cf55a13b754539906582ec8b174bd58d5d1f3d767c613721ae05":16:"010001":MBEDTLS_MD_SHA1:MBEDTL
S_MD_SHA1:"25f10895a87716c137450bb9519dfaa1f207faa942ea88abf71e9c17980085b555aebab76264ae2a3ab9
3c2d12981191ddac6fb5949eb36aee3c5da940f00752c916d94608fa7d97ba6a2915b688f20323d4e9d96801d89a72ab
5892dc2117c07434fcf972e058cf8c41ca4b4ff554f7d5068ad3155fced0f3125bc04f9193378a8f5c4c3b8cb4dd6d1cc6
9d30ecca6eaa51e36a05730e9e342e855baf099defb8afd7":"ad8b1523703646224b660b550885917ca2d1df28":"6d3b
5b87f67ea657af21f75441977d2180f91b2c5f692de82955696a686730d9b9778d970758ccb26071c2209ffbd6125be2e
96ea81b67cb9b9308239fda17f7b2b64ecda096b6b935640a5a1cb42a9155b1c9ef7a633a02c59f0d6ee59b852c43b350
29e73c940ff0410e8f114eed46bbd0fae165e42be2528a401c3b28fd818ef3232dca9f4d2a0f5166ec59c42396d6c11dbc
1215a56fa17169db9575343ef34f9de32a49cdc3174922f229c23e18e45df9353119ec4319cedce7a17c64088c1f6f52be
29634100b3919d38f3d1ed94e6891e66a73b8fb849f5874df59459e298c7bbce2eee782a195aa66fe2d0732b25e595f57
d3e061b1fc3e4063bf98f":0

RSASSA-PSS
Signature verify options #1 (OK)
pkcs1_rsassa_pss_verify_ext:2048:16:"a5dd867ac4cb02f90b9457d48c14a770ef991c56c39c0ec65fd11afa8937cea57
b9be7ac73b45c0017615b82d622e318753b6027c0fd157be12f8090fee2a7adcd0eef759f88ba4997c7a42d58c9aa12cb
99ae001fe521c13bb5431445a8d5ae4f5e4c7e948ac227d3604071f20e577e905fbeb15dfaf06d1de5ae6253d63a6a212
0b31a5da5dabc9550600e20f27d3739e2627925fea3cc509f21dff04e6eea4549c540d6809ff9307eede91fff58733d838
5a237d6d3705a33e391900992070df7adf1357cf7e3700ce3667de83f17b8df1778db381dce09cb4ad058a511001a738
198ee27cf55a13b754539906582ec8b174bd58d5d1f3d767c613721ae05":16:"010001":MBEDTLS_MD_SHA1:MB
EDTLS_MD_SHA1:MBEDTLS_MD_SHA1:20:"25f10895a87716c137450bb9519dfaa1f207faa942ea88abf71e9c17
980085b555aebab76264ae2a3ab93c2d12981191ddac6fb5949eb36aee3c5da940f00752c916d94608fa7d97ba6a2915
b688f20323d4e9d96801d89a72ab5892dc2117c07434fcf972e058cf8c41ca4b4ff554f7d5068ad3155fced0f3125bc04f
9193378a8f5c4c3b8cb4dd6d1cc69d30ecca6eaa51e36a05730e9e342e855baf099defb8afd7":"6d3b5b87f67ea657af21
f75441977d2180f91b2c5f692de82955696a686730d9b9778d970758ccb26071c2209ffbd6125be2e96ea81b67cb9b93
08239fda17f7b2b64ecda096b6b935640a5a1cb42a9155b1c9ef7a633a02c59f0d6ee59b852c43b35029e73c940ff0410
e8f114eed46bbd0fae165e42be2528a401c3b28fd818ef3232dca9f4d2a0f5166ec59c42396d6c11dbc1215a56fa17169d
b9575343ef34f9de32a49cdc3174922f229c23e18e45df9353119ec4319cedce7a17c64088c1f6f52be29634100b3919d
38f3d1ed94e6891e66a73b8fb849f5874df59459e298c7bbce2eee782a195aa66fe2d0732b25e595f57d3e061b1fc3e406
3bf98f":0:0

RSASSA-PSS
Signature verify options #2 (ctx_hash none)
pkcs1_rsassa_pss_verify_ext:2048:16:"a5dd867ac4cb02f90b9457d48c14a770ef991c56c39c0ec65fd11afa8937cea57
b9be7ac73b45c0017615b82d622e318753b6027c0fd157be12f8090fee2a7adcd0eef759f88ba4997c7a42d58c9aa12cb
99ae001fe521c13bb5431445a8d5ae4f5e4c7e948ac227d3604071f20e577e905fbeb15dfaf06d1de5ae6253d63a6a212
0b31a5da5dabc9550600e20f27d3739e2627925fea3cc509f21dff04e6eea4549c540d6809ff9307eede91fff58733d838
5a237d6d3705a33e391900992070df7adf1357cf7e3700ce3667de83f17b8df1778db381dce09cb4ad058a511001a738
198ee27cf55a13b754539906582ec8b174bd58d5d1f3d767c613721ae05":16:"010001":MBEDTLS_MD_SHA1:MB
EDTLS_MD_NONE:MBEDTLS_MD_SHA1:20:"25f10895a87716c137450bb9519dfaa1f207faa942ea88abf71e9c1
7980085b555aebab76264ae2a3ab93c2d12981191ddac6fb5949eb36aee3c5da940f00752c916d94608fa7d97ba6a291
5b688f20323d4e9d96801d89a72ab5892dc2117c07434fcf972e058cf8c41ca4b4ff554f7d5068ad3155fced0f3125bc04
f9193378a8f5c4c3b8cb4dd6d1cc69d30ecca6eaa51e36a05730e9e342e855baf099defb8afd7":"6d3b5b87f67ea657af2
1f75441977d2180f91b2c5f692de82955696a686730d9b9778d970758ccb26071c2209ffbd6125be2e96ea81b67cb9b9
308239fda17f7b2b64ecda096b6b935640a5a1cb42a9155b1c9ef7a633a02c59f0d6ee59b852c43b35029e73c940ff041
0e8f114eed46bbd0fae165e42be2528a401c3b28fd818ef3232dca9f4d2a0f5166ec59c42396d6c11dbc1215a56fa17169
db9575343ef34f9de32a49cdc3174922f229c23e18e45df9353119ec4319cedce7a17c64088c1f6f52be29634100b3919
d38f3d1ed94e6891e66a73b8fb849f5874df59459e298c7bbce2eee782a195aa66fe2d0732b25e595f57d3e061b1fc3e40
63bf98f":0:0

RSASSA-PSS
Signature verify options #3 (ctx_hash diverging)
depends_on:MBEDTLS_SHA256_C
pkcs1_rsassa_pss_verify_ext:2048:16:"a5dd867ac4cb02f90b9457d48c14a770ef991c56c39c0ec65fd11afa8937cea57
b9be7ac73b45c0017615b82d622e318753b6027c0fd157be12f8090fee2a7adcd0eef759f88ba4997c7a42d58c9aa12cb
99ae001fe521c13bb5431445a8d5ae4f5e4c7e948ac227d3604071f20e577e905fbeb15dfaf06d1de5ae6253d63a6a212
0b31a5da5dabc9550600e20f27d3739e2627925fea3cc509f21dff04e6eea4549c540d6809ff9307eede91fff58733d838
5a237d6d3705a33e391900992070df7adf1357cf7e3700ce3667de83f17b8df1778db381dce09cb4ad058a511001a738
198ee27cf55a13b754539906582ec8b174bd58d5d1f3d767c613721ae05":16:"010001":MBEDTLS_MD_SHA1:MB
EDTLS_MD_SHA256:MBEDTLS_MD_SHA1:20:"25f10895a87716c137450bb9519dfaa1f207faa942ea88abf71e9c
17980085b555aebab76264ae2a3ab93c2d12981191ddac6fb5949eb36aee3c5da940f00752c916d94608fa7d97ba6a29
15b688f20323d4e9d96801d89a72ab5892dc2117c07434fcf972e058cf8c41ca4b4ff554f7d5068ad3155fced0f3125bc0
4f9193378a8f5c4c3b8cb4dd6d1cc69d30ecca6eaa51e36a05730e9e342e855baf099defb8afd7":"6d3b5b87f67ea657af
21f75441977d2180f91b2c5f692de82955696a686730d9b9778d970758ccb26071c2209ffbd6125be2e96ea81b67cb9b
9308239fda17f7b2b64ecda096b6b935640a5a1cb42a9155b1c9ef7a633a02c59f0d6ee59b852c43b35029e73c940ff04
10e8f114eed46bbd0fae165e42be2528a401c3b28fd818ef3232dca9f4d2a0f5166ec59c42396d6c11dbc1215a56fa1716
9db9575343ef34f9de32a49cdc3174922f229c23e18e45df9353119ec4319cedce7a17c64088c1f6f52be29634100b391
9d38f3d1ed94e6891e66a73b8fb849f5874df59459e298c7bbce2eee782a195aa66fe2d0732b25e595f57d3e061b1fc3e4
063bf98f":MBEDTLS_ERR_RSA_INVALID_PADDING:0

RSASSA-PSS
Signature verify options #4 (mgf1_hash diverging)
depends_on:MBEDTLS_SHA256_C
pkcs1_rsassa_pss_verify_ext:2048:16:"a5dd867ac4cb02f90b9457d48c14a770ef991c56c39c0ec65fd11afa8937cea57
b9be7ac73b45c0017615b82d622e318753b6027c0fd157be12f8090fee2a7adcd0eef759f88ba4997c7a42d58c9aa12cb
99ae001fe521c13bb5431445a8d5ae4f5e4c7e948ac227d3604071f20e577e905fbeb15dfaf06d1de5ae6253d63a6a212
0b31a5da5dabc9550600e20f27d3739e2627925fea3cc509f21dff04e6eea4549c540d6809ff9307eede91fff58733d838
5a237d6d3705a33e391900992070df7adf1357cf7e3700ce3667de83f17b8df1778db381dce09cb4ad058a511001a738
198ee27cf55a13b754539906582ec8b174bd58d5d1f3d767c613721ae05":16:"010001":MBEDTLS_MD_SHA1:MB

EDTLS_MD_SHA1:MBEDTLS_MD_SHA256:20:"25f10895a87716c137450bb9519dfaa1f207faa942ea88abf71e9c
17980085b555aebab76264ae2a3ab93c2d12981191ddac6fb5949eb36aee3c5da940f00752c916d94608fa7d97ba6a29
15b688f20323d4e9d96801d89a72ab5892dc2117c07434fcf972e058cf8c41ca4b4ff554f7d5068ad3155fced0f3125bc0
4f9193378a8f5c4c3b8cb4dd6d1cc69d30ecca6eaa51e36a05730e9e342e855baf099defb8afd7":"6d3b5b87f67ea657af
21f75441977d2180f91b2c5f692de82955696a686730d9b9778d970758ccb26071c2209ffbd6125be2e96ea81b67cb9b
9308239fda17f7b2b64ecda096b6b935640a5a1cb42a9155b1c9ef7a633a02c59f0d6ee59b852c43b35029e73c940ff04
10e8f114eed46bbd0fae165e42be2528a401c3b28fd818ef3232dca9f4d2a0f5166ec59c42396d6c11dbc1215a56fa1716
9db9575343ef34f9de32a49cdc3174922f229c23e18e45df9353119ec4319cedce7a17c64088c1f6f52be29634100b391
9d38f3d1ed94e6891e66a73b8fb849f5874df59459e298c7bbce2eee782a195aa66fe2d0732b25e595f57d3e061b1fc3e4
063bf98f":0:MBEDTLS_ERR_RSA_INVALID_PADDING

RSASSA-PSS
Signature verify options #5 (wrong msg_hash)
depends_on:MBEDTLS_SHA256_C
pkcs1_rsassa_pss_verify_ext:2048:16:"a5dd867ac4cb02f90b9457d48c14a770ef991c56c39c0ec65fd11afa8937cea57
b9be7ac73b45c0017615b82d622e318753b6027c0fd157be12f8090fee2a7adcd0eef759f88ba4997c7a42d58c9aa12cb
99ae001fe521c13bb5431445a8d5ae4f5e4c7e948ac227d3604071f20e577e905fbeb15dfaf06d1de5ae6253d63a6a212
0b31a5da5dabc9550600e20f27d3739e2627925fea3cc509f21dff04e6eea4549c540d6809ff9307eede91fff58733d838
5a237d6d3705a33e391900992070df7adf1357cf7e3700ce3667de83f17b8df1778db381dce09cb4ad058a511001a738
198ee27cf55a13b754539906582ec8b174bd58d5d1f3d767c613721ae05":16:"010001":MBEDTLS_MD_SHA256:M
BEDTLS_MD_SHA1:MBEDTLS_MD_SHA1:20:"25f10895a87716c137450bb9519dfaa1f207faa942ea88abf71e9c
17980085b555aebab76264ae2a3ab93c2d12981191ddac6fb5949eb36aee3c5da940f00752c916d94608fa7d97ba6a29
15b688f20323d4e9d96801d89a72ab5892dc2117c07434fcf972e058cf8c41ca4b4ff554f7d5068ad3155fced0f3125bc0
4f9193378a8f5c4c3b8cb4dd6d1cc69d30ecca6eaa51e36a05730e9e342e855baf099defb8afd7":"6d3b5b87f67ea657af
21f75441977d2180f91b2c5f692de82955696a686730d9b9778d970758ccb26071c2209ffbd6125be2e96ea81b67cb9b
9308239fda17f7b2b64ecda096b6b935640a5a1cb42a9155b1c9ef7a633a02c59f0d6ee59b852c43b35029e73c940ff04
10e8f114eed46bbd0fae165e42be2528a401c3b28fd818ef3232dca9f4d2a0f5166ec59c42396d6c11dbc1215a56fa1716
9db9575343ef34f9de32a49cdc3174922f229c23e18e45df9353119ec4319cedce7a17c64088c1f6f52be29634100b391
9d38f3d1ed94e6891e66a73b8fb849f5874df59459e298c7bbce2eee782a195aa66fe2d0732b25e595f57d3e061b1fc3e4
063bf98f":MBEDTLS_ERR_RSA_VERIFY_FAILED:MBEDTLS_ERR_RSA_VERIFY_FAILED

RSASSA-PSS
Signature verify options #6 (wrong expected_salt_len)
pkcs1_rsassa_pss_verify_ext:2048:16:"a5dd867ac4cb02f90b9457d48c14a770ef991c56c39c0ec65fd11afa8937cea57
b9be7ac73b45c0017615b82d622e318753b6027c0fd157be12f8090fee2a7adcd0eef759f88ba4997c7a42d58c9aa12cb
99ae001fe521c13bb5431445a8d5ae4f5e4c7e948ac227d3604071f20e577e905fbeb15dfaf06d1de5ae6253d63a6a212
0b31a5da5dabc9550600e20f27d3739e2627925fea3cc509f21dff04e6eea4549c540d6809ff9307eede91fff58733d838
5a237d6d3705a33e391900992070df7adf1357cf7e3700ce3667de83f17b8df1778db381dce09cb4ad058a511001a738
198ee27cf55a13b754539906582ec8b174bd58d5d1f3d767c613721ae05":16:"010001":MBEDTLS_MD_SHA1:MB
EDTLS_MD_SHA1:MBEDTLS_MD_SHA1:21:"25f10895a87716c137450bb9519dfaa1f207faa942ea88abf71e9c17
980085b555aebab76264ae2a3ab93c2d12981191ddac6fb5949eb36aee3c5da940f00752c916d94608fa7d97ba6a2915
b688f20323d4e9d96801d89a72ab5892dc2117c07434fcf972e058cf8c41ca4b4ff554f7d5068ad3155fced0f3125bc04f
9193378a8f5c4c3b8cb4dd6d1cc69d30ecca6eaa51e36a05730e9e342e855baf099defb8afd7":"6d3b5b87f67ea657af21
f75441977d2180f91b2c5f692de82955696a686730d9b9778d970758ccb26071c2209ffbd6125be2e96ea81b67cb9b93
08239fda17f7b2b64ecda096b6b935640a5a1cb42a9155b1c9ef7a633a02c59f0d6ee59b852c43b35029e73c940ff0410
e8f114eed46bbd0fae165e42be2528a401c3b28fd818ef3232dca9f4d2a0f5166ec59c42396d6c11dbc1215a56fa17169d
b9575343ef34f9de32a49cdc3174922f229c23e18e45df9353119ec4319cedce7a17c64088c1f6f52be29634100b3919d
38f3d1ed94e6891e66a73b8fb849f5874df59459e298c7bbce2eee782a195aa66fe2d0732b25e595f57d3e061b1fc3e406

3bf98f":0:MBEDTLS_ERR_RSA_INVALID_PADDING

RSASSA-PSS
Signature verify options #7 (wrong expected_salt_len)
pkcs1_rsassa_pss_verify_ext:2048:16:"a5dd867ac4cb02f90b9457d48c14a770ef991c56c39c0ec65fd11afa8937cea57
b9be7ac73b45c0017615b82d622e318753b6027c0fd157be12f8090fee2a7adcd0eef759f88ba4997c7a42d58c9aa12cb
99ae001fe521c13bb5431445a8d5ae4f5e4c7e948ac227d3604071f20e577e905fbeb15dfaf06d1de5ae6253d63a6a212
0b31a5da5dabc9550600e20f27d3739e2627925fea3cc509f21dff04e6eea4549c540d6809ff9307eede91fff58733d838
5a237d6d3705a33e391900992070df7adf1357cf7e3700ce3667de83f17b8df1778db381dce09cb4ad058a511001a738
198ee27cf55a13b754539906582ec8b174bd58d5d1f3d767c613721ae05":16:"010001":MBEDTLS_MD_SHA1:MB
EDTLS_MD_SHA1:MBEDTLS_MD_SHA1:19:"25f10895a87716c137450bb9519dfaa1f207faa942ea88abf71e9c17
980085b555aebab76264ae2a3ab93c2d12981191ddac6fb5949eb36aee3c5da940f00752c916d94608fa7d97ba6a2915
b688f20323d4e9d96801d89a72ab5892dc2117c07434fcf972e058cf8c41ca4b4ff554f7d5068ad3155fced0f3125bc04f
9193378a8f5c4c3b8cb4dd6d1cc69d30ecca6eaa51e36a05730e9e342e855baf099defb8afd7":"6d3b5b87f67ea657af21
f75441977d2180f91b2c5f692de82955696a686730d9b9778d970758ccb26071c2209ffbd6125be2e96ea81b67cb9b93
08239fda17f7b2b64ecda096b6b935640a5a1cb42a9155b1c9ef7a633a02c59f0d6ee59b852c43b35029e73c940ff0410
e8f114eed46bbd0fae165e42be2528a401c3b28fd818ef3232dca9f4d2a0f5166ec59c42396d6c11dbc1215a56fa17169d
b9575343ef34f9de32a49cdc3174922f229c23e18e45df9353119ec4319cedce7a17c64088c1f6f52be29634100b3919d
38f3d1ed94e6891e66a73b8fb849f5874df59459e298c7bbce2eee782a195aa66fe2d0732b25e595f57d3e061b1fc3e406
3bf98f":0:MBEDTLS_ERR_RSA_INVALID_PADDING

RSASSA-PSS
Signature verify options #8 (non-default salt_len: max)
depends_on:MBEDTLS_SHA256_C
pkcs1_rsassa_pss_verify_ext:1024:16:"00dd118a9f99bab068ca2aea3b6a6d5997ed4ec954e40deecea07da01eaae80e
c2bb1340db8a128e891324a5c5f5fad8f590d7c8cacbc5fe931dafda1223735279461abaa0572b761631b3a8afe7389b0
88b63993a0a25ee45d21858bab9931aedd4589a631b37fcf714089f856549f359326dd1e0e86dde52ed66b4a90bda409
5":16:"010001":MBEDTLS_MD_SHA256:MBEDTLS_MD_SHA256:MBEDTLS_MD_SHA256:94:"5465737420
6d657373616765":"0d2bdb0456a3d651d5bd48a4204493898f72cf1aaddd71387cc058bc3f4c235ea6be4010fd61b28e
1fbb275462b53775c04be9022d38b6a2e0387dddba86a3f8554d2858044a59fddbd594753fc056fe33c8daddb85dc70d
164690b1182209ff84824e0be10e35c379f2f378bf176a9f7cb94d95e44d90276a298c8810f741c9":0:0

RSASSA-PSS
Signature verify options #9 (non-default salt_len: 0)
depends_on:MBEDTLS_SHA256_C
pkcs1_rsassa_pss_verify_ext:1024:16:"00dd118a9f99bab068ca2aea3b6a6d5997ed4ec954e40deecea07da01eaae80e
c2bb1340db8a128e891324a5c5f5fad8f590d7c8cacbc5fe931dafda1223735279461abaa0572b761631b3a8afe7389b0
88b63993a0a25ee45d21858bab9931aedd4589a631b37fcf714089f856549f359326dd1e0e86dde52ed66b4a90bda409
5":16:"010001":MBEDTLS_MD_SHA256:MBEDTLS_MD_SHA256:MBEDTLS_MD_SHA256:0:"54657374206
d657373616765":"7fc506d26ca3b22922a1ce39faaedd273161b82d9443c56f1a034f131ae4a18cae1474271cb4b66a1
7d9707ca58b0bdbd3c406b7e65bbcc9bbbce94dc45de807b4989b23b3e4db74ca29298137837eb90cc83d3219249bc7
d480fceaf075203a86e54c4ecfa4e312e39f8f69d76534089a36ed9049ca9cfd5ab1db1fa75fe5c8":0:0

RSASSA-PSS
Signature verify options #10 (non-default salt_len: 0, ANY)
depends_on:MBEDTLS_SHA256_C
pkcs1_rsassa_pss_verify_ext:1024:16:"00dd118a9f99bab068ca2aea3b6a6d5997ed4ec954e40deecea07da01eaae80e
c2bb1340db8a128e891324a5c5f5fad8f590d7c8cacbc5fe931dafda1223735279461abaa0572b761631b3a8afe7389b0

88b63993a0a25ee45d21858bab9931aedd4589a631b37fcf714089f856549f359326dd1e0e86dde52ed66b4a90bda409
5":16:"010001":MBEDTLS_MD_SHA256:MBEDTLS_MD_SHA256:MBEDTLS_MD_SHA256:MBEDTLS_RS
A_SALT_LEN_ANY:"54657374206d657373616765":"7fc506d26ca3b22922a1ce39faaedd273161b82d9443c56f1a
034f131ae4a18cae1474271cb4b66a17d9707ca58b0bdbd3c406b7e65bbcc9bbbce94dc45de807b4989b23b3e4db74ca
29298137837eb90cc83d3219249bc7d480fceaf075203a86e54c4ecfa4e312e39f8f69d76534089a36ed9049ca9cfd5ab
1db1fa75fe5c8":0:0

RSASSA-PSS
Signature verify options #11 (MGF1 alg != MSG hash alg)
depends_on:MBEDTLS_SHA256_C
pkcs1_rsassa_pss_verify_ext:1024:16:"00dd118a9f99bab068ca2aea3b6a6d5997ed4ec954e40deecea07da01eaae80e
c2bb1340db8a128e891324a5c5f5fad8f590d7c8cacbc5fe931dafda1223735279461abaa0572b761631b3a8afe7389b0
88b63993a0a25ee45d21858bab9931aedd4589a631b37fcf714089f856549f359326dd1e0e86dde52ed66b4a90bda409
5":16:"010001":MBEDTLS_MD_NONE:MBEDTLS_MD_SHA256:MBEDTLS_MD_SHA256:MBEDTLS_RSA_
SALT_LEN_ANY:"c0719e9a8d5d838d861dc6f675c899d2b309a3a65bb9fe6b11e5afcbf9a2c0b1":"7fc506d26ca3b2
2922a1ce39faaedd273161b82d9443c56f1a034f131ae4a18cae1474271cb4b66a17d9707ca58b0bdbd3c406b7e65bbcc
9bbbce94dc45de807b4989b23b3e4db74ca29298137837eb90cc83d3219249bc7d480fceaf075203a86e54c4ecfa4e31
2e39f8f69d76534089a36ed9049ca9cfd5ab1db1fa75fe5c8":0:0

RSASSA-PSS Signature verify options #12 (MGF1 alg != MSG hash alg, ctx wrong)
depends_on:MBEDTLS_SHA256_C
pkcs1_rsassa_pss_verify_ext:1024:16:"00dd118a9f99bab068ca2aea3b6a6d5997ed4ec954e40deecea07da01eaae80e
c2bb1340db8a128e891324a5c5f5fad8f590d7c8cacbc5fe931dafda1223735279461abaa0572b761631b3a8afe7389b0
88b63993a0a25ee45d21858bab9931aedd4589a631b37fcf714089f856549f359326dd1e0e86dde52ed66b4a90bda409
5":16:"010001":MBEDTLS_MD_NONE:MBEDTLS_MD_SHA1:MBEDTLS_MD_SHA256:MBEDTLS_RSA_S
ALT_LEN_ANY:"c0719e9a8d5d838d861dc6f675c899d2b309a3a65bb9fe6b11e5afcbf9a2c0b1":"7fc506d26ca3b22
922a1ce39faaedd273161b82d9443c56f1a034f131ae4a18cae1474271cb4b66a17d9707ca58b0bdbd3c406b7e65bbcc9
bbbce94dc45de807b4989b23b3e4db74ca29298137837eb90cc83d3219249bc7d480fceaf075203a86e54c4ecfa4e312e
39f8f69d76534089a36ed9049ca9cfd5ab1db1fa75fe5c8":MBEDTLS_ERR_RSA_INVALID_PADDING:0

RSASSA-PSS
Signature verify options #13 (MGF1 alg != MSG hash alg, arg wrong)
depends_on:MBEDTLS_SHA256_C
pkcs1_rsassa_pss_verify_ext:1024:16:"00dd118a9f99bab068ca2aea3b6a6d5997ed4ec954e40deecea07da01eaae80e
c2bb1340db8a128e891324a5c5f5fad8f590d7c8cacbc5fe931dafda1223735279461abaa0572b761631b3a8afe7389b0
88b63993a0a25ee45d21858bab9931aedd4589a631b37fcf714089f856549f359326dd1e0e86dde52ed66b4a90bda409
5":16:"010001":MBEDTLS_MD_NONE:MBEDTLS_MD_SHA256:MBEDTLS_MD_SHA1:MBEDTLS_RSA_S
ALT_LEN_ANY:"c0719e9a8d5d838d861dc6f675c899d2b309a3a65bb9fe6b11e5afcbf9a2c0b1":"7fc506d26ca3b22
922a1ce39faaedd273161b82d9443c56f1a034f131ae4a18cae1474271cb4b66a17d9707ca58b0bdbd3c406b7e65bbcc9
bbbce94dc45de807b4989b23b3e4db74ca29298137837eb90cc83d3219249bc7d480fceaf075203a86e54c4ecfa4e312e
39f8f69d76534089a36ed9049ca9cfd5ab1db1fa75fe5c8":0:MBEDTLS_ERR_RSA_INVALID_PADDING
-----BEGIN X509 CRL-----
MIIBcTCB9wIBATAKBggqhkjOPQQDAjA+MQswCQYDVQQGEwJOTDERMA8GA1UEChMI
UG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EXDTEzMDkyNDE2
MzEwOFoXDTIzMDkyMjE2MzEwOFowFDASAgEKFw0xMzA5MjQxNjI4MzhaoHIwcDBu
BgNVHSMEZzBlgBSdbSAkSQE/K8t4tRm8fiTJ2/s2fKFCpEAwPjELMAkGA1UEBhMC
TkwxETAPBgNVBAoTCFBvbGFyU1NMMRwwGgYDVQQDExNQb2xhcnNzbCBUZXN0IEVD
IENBggkAwUPifmJDzOgwCgYIKoZIzj0EAwIDaQAwZgIxAKuQ684s7gyhtxKJr6Ln

```
S2BQ02f1jjPHrZVdXaZvm3C5tGi2cKkoK1aMiyC3LsRCuAIxAIMhj0TmcuIZr5fX
g5RByD7zUnZBpoEAdgxFy4JPJ2IViWOPekSGh8b/JY1VNS6Zbw==
-----END X509 CRL-----
-----BEGIN CERTIFICATE-----
MIIB6TCCAW+gAwIBAgIBOzAKBggqhkjOPQQDAjA+MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EwHhcN
MTQwNDEwMTcyMDU4WhcNMjQwNDA3MTcyMDU4WjA0MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxEjAQBgNVBAMTCWxvY2FsaG9zdDBZMBMGByqGSM49AgEG
CCqGSM49AwEHA0IABDfMVtl2CR5acj7HWS3/IG7ufPkGkXTQrRS192giWWKSTuUA
2CMR/+ov0jRdXRa9iojCa3cNVc2KKg76Aci07f+jaDBmMAkGA1UdEwQCMAAwHQYD
VR0OBBYEFFBhpY/UB9nXggEM5WV/jGNGpxO+MB8GA1UdIwQYMBaAFJ1tICRJAT8r
y3i1Gbx+JMnb+zZ8MBkGA1UdJQQSMBAGCCsGAQUFBwMDBgRVHSUAMAoGCCqGSM49
BAMCA2gAMGUCMQCSYaq/9IKOTkzIrU/eOtpha/3af3JwT6vKh4N3cSX62ksMz0GT
Uxmq4UGMBt4VmBkCMBGpYqof6hS1o92ltNRpDSHuVQ+nke1lOsoQ1plZp4SI+bY1
bUD/WrUSLlwikZAeng==
-----END CERTIFICATE-----
set(libs
  mbedtls
)

add_executable(strerror strerror.c)
target_link_libraries(strerror ${libs})

add_executable(pem2der pem2der.c)
target_link_libraries(pem2der ${libs})

install(TARGETS strerror pem2der
    DESTINATION "bin"
    PERMISSIONS OWNER_READ OWNER_WRITE OWNER_EXECUTE GROUP_READ
GROUP_EXECUTE WORLD_READ WORLD_EXECUTE)
Test case mbedtls_base64_encode #1 buffer just right
mbedtls_base64_encode:"":"":0:0

Test case mbedtls_base64_encode #2 buffer just right
mbedtls_base64_encode:"f":"Zg==":5:0

Test case mbedtls_base64_encode #2 buffer too small
mbedtls_base64_encode:"f":"Zg==":4:MBEDTLS_ERR_BASE64_BUFFER_TOO_SMALL

Test case mbedtls_base64_encode #3 buffer just right
mbedtls_base64_encode:"fo":"Zm8=":5:0

Test case mbedtls_base64_encode #3 buffer too small
mbedtls_base64_encode:"fo":"Zm8=":4:MBEDTLS_ERR_BASE64_BUFFER_TOO_SMALL

Test case mbedtls_base64_encode #4 buffer just right
mbedtls_base64_encode:"foo":"Zm9v":5:0
```

Test case mbedtls_base64_encode #4 buffer too small
mbedtls_base64_encode:"foo":"Zm9v":4:MBEDTLS_ERR_BASE64_BUFFER_TOO_SMALL

Test case mbedtls_base64_encode #5 buffer just right
mbedtls_base64_encode:"foob":"Zm9vYg==":9:0

Test case mbedtls_base64_encode #5 buffer too small
mbedtls_base64_encode:"foob":"Zm9vYg==":8:MBEDTLS_ERR_BASE64_BUFFER_TOO_SMALL

Test case mbedtls_base64_encode #6
buffer just right
mbedtls_base64_encode:"fooba":"Zm9vYmE=":9:0

Test case mbedtls_base64_encode #6 buffer too small
mbedtls_base64_encode:"fooba":"Zm9vYmE=":8:MBEDTLS_ERR_BASE64_BUFFER_TOO_SMALL

Test case mbedtls_base64_encode #7 buffer just right
mbedtls_base64_encode:"foobar":"Zm9vYmFy":9:0

Test case mbedtls_base64_encode #7 buffer too small
mbedtls_base64_encode:"foobar":"Zm9vYmFy":8:MBEDTLS_ERR_BASE64_BUFFER_TOO_SMALL

Test case mbedtls_base64_decode #1
mbedtls_base64_decode:"":"":0

Test case mbedtls_base64_decode #2
mbedtls_base64_decode:"Zg==":"f":0

Test case mbedtls_base64_decode #3
mbedtls_base64_decode:"Zm8=":"fo":0

Test case mbedtls_base64_decode #4
mbedtls_base64_decode:"Zm9v":"foo":0

Test case mbedtls_base64_decode #5
mbedtls_base64_decode:"Zm9vYg==":"foob":0

Test case mbedtls_base64_decode #6
mbedtls_base64_decode:"Zm9vYmE=":"fooba":0

Test case mbedtls_base64_decode #7
mbedtls_base64_decode:"Zm9vYmFy":"foobar":0

Base64 decode (Illegal character)
mbedtls_base64_decode:"zm#=":"":MBEDTLS_ERR_BASE64_INVALID_CHARACTER

Base64

decode (Too much equal signs)
mbedtls_base64_decode:"zm===":"":MBEDTLS_ERR_BASE64_INVALID_CHARACTER

Base64 decode (Invalid char after equal signs)
mbedtls_base64_decode:"zm=masd":"":MBEDTLS_ERR_BASE64_INVALID_CHARACTER

Base64 decode (Space inside string)
mbedtls_base64_decode:"zm masd":"":MBEDTLS_ERR_BASE64_INVALID_CHARACTER

Base64 decode "Zm9vYmFy" (no newline nor '\0' at end)
base64_decode_hex_src:"5a6d3976596d4679":"foobar":0

Base64 decode "Zm9vYmFy\n" (LF at end)
base64_decode_hex_src:"5a6d3976596d46790a":"foobar":0

Base64 decode "Zm9vYmFy\r\n" (CRLF at end)
base64_decode_hex_src:"5a6d3976596d46790d0a":"foobar":0

Base64 decode "Zm9vYmFy\r" (CR at end)
base64_decode_hex_src:"5a6d3976596d46790d":"":MBEDTLS_ERR_BASE64_INVALID_CHARACTER

Base64 decode "Zm9vYmFy " (SP at end)
base64_decode_hex_src:"5a6d3976596d467920":"foobar":0

Base64 decode "Zm9vYmFy \n" (SP+LF at end)
base64_decode_hex_src:"5a6d3976596d4679200a":"foobar":0

Base64
decode "Zm9vYmFy \r\n" (SP+CRLF at end)
base64_decode_hex_src:"5a6d3976596d4679200d0a":"foobar":0

Base64 decode "Zm9vYmFy \r" (SP+CR at end)
base64_decode_hex_src:"5a6d3976596d4679200d":"":MBEDTLS_ERR_BASE64_INVALID_CHARACTER

Base64 decode "Zm9vYmFy " (2SP at end)
base64_decode_hex_src:"5a6d3976596d46792020":"foobar":0

Base64 decode "Zm9vYmFy \n" (2SP+LF at end)
base64_decode_hex_src:"5a6d3976596d467920200a":"foobar":0

Base64 decode "Zm9vYmFy \r\n" (2SP+CRLF at end)
base64_decode_hex_src:"5a6d3976596d467920200d0a":"foobar":0

Base64 decode "Zm9vYmFy \r" (2SP+CR at end)
base64_decode_hex_src:"5a6d3976596d467920200d":"":MBEDTLS_ERR_BASE64_INVALID_CHARACTER

Base64 decode "Zm9vYmF\ny" (LF inside)
base64_decode_hex_src:"5a6d3976596d460a79":"foobar":0

Base64 decode "Zm9vYmF\ry" (CRLF inside)
base64_decode_hex_src:"5a6d3976596d460d0a79":"foobar":0

Base64 decode "Zm9vYmF\ry" (CR inside)
base64_decode_hex_src:"5a6d3976596d460d79":"":MBEDTLS_ERR_BASE64_INVALID_CHARACTER

Base64
decode "Zm9vYmF y" (SP inside)
base64_decode_hex_src:"5a6d3976596d462079":"":MBEDTLS_ERR_BASE64_INVALID_CHARACTER

Base64 decode "Zm9vYmF \ny" (SP+LF inside)
base64_decode_hex_src:"5a6d3976596d46200a79":"foobar":0

Base64 decode "Zm9vYmF \ry" (SP+CRLF inside)
base64_decode_hex_src:"5a6d3976596d46200d0a79":"foobar":0

Base64 decode "Zm9vYmF \ry" (SP+CR inside)
base64_decode_hex_src:"5a6d3976596d46200d79":"":MBEDTLS_ERR_BASE64_INVALID_CHARACTER

Base64 decode "Zm9vYmF y" (2SP inside)
base64_decode_hex_src:"5a6d3976596d46202079":"":MBEDTLS_ERR_BASE64_INVALID_CHARACTER

Base64 decode "Zm9vYmF \ny" (2SP+LF inside)
base64_decode_hex_src:"5a6d3976596d4620200a79":"foobar":0

Base64 decode "Zm9vYmF \ry" (2SP+CRLF inside)
base64_decode_hex_src:"5a6d3976596d4620200d0a79":"foobar":0

Base64 decode "Zm9vYmF \ry" (2SP+CR inside)
base64_decode_hex_src:"5a6d3976596d4620200d79":"":MBEDTLS_ERR_BASE64_INVALID_CHARACTER

Base64 encode hex #1
base64_encode_hex:"010203040506070809":"AQIDBAUGBwgJ":13:0

Base64
encode hex #2 (buffer too small)
base64_encode_hex:"010203040506070809":"AQIDBAUGBwgJ":12:MBEDTLS_ERR_BASE64_BUFFER_TOO
_SMALL

Base64 encode hex #3
base64_encode_hex:"0102030405060708":"AQIDBAUGBwg=":13:0

Base64 encode hex #4
base64_encode_hex:"01020304050607":"AQIDBAUGBw==":13:0

Base64 decode hex #1
base64_decode_hex:"AQIDBAUGBwgJ":"010203040506070809":9:0

Base64 decode hex #2 (buffer too small)
base64_decode_hex:"AQIDBAUGBwgJ":"010203040506070809":8:MBEDTLS_ERR_BASE64_BUFFER_TOO_SMALL

Base64 decode hex #3
base64_decode_hex:"AQIDBAUGBwg=":"0102030405060708":8:0

Base64 decode hex #4
base64_decode_hex:"AQIDBAUGBw==":"01020304050607":7:0

Base64 decode hex #5 (buffer too small)
base64_decode_hex:"AQIDBAUGBw==":"01020304050607":6:MBEDTLS_ERR_BASE64_BUFFER_TOO_SMALL

Base64 Selftest
depends_on:MBEDTLS_SELF_TEST
base64_selftest:
This documents the X.509 CAs, certificates, and CRLS used for testing.

Certification authorities

There are two main CAs for use as trusted roots:
- test-ca.crt aka "C=NL, O=PolarSSL, CN=PolarSSL Test CA"
 uses a RSA-2048 key
 test-ca-sha1.crt and test-ca-sha256.crt use the same key, signed with
 different hashes.
- test-ca2*.crt aka "C=NL, O=PolarSSL, CN=Polarssl Test EC CA"
 uses an EC key with NIST P-384 (aka secp384r1)
 variants used to test the keyUsage extension
The files test-ca_cat12 and test-ca_cat21 contain them concatenated both ways.

Two intermediate CAs are signed by them:
- test-int-ca.crt "C=NL, O=PolarSSL, CN=PolarSSL Test Intermediate CA"
 uses RSA-4096, signed by test-ca2
- test-int-ca2.crt "C=NL, O=PolarSSL, CN=PolarSSL Test Intermediate EC CA"
 uses an EC key with NIST P-256, signed by test-ca

A third intermediate CA is signed by test-int-ca2.crt:
- test-int-ca3.crt "C=UK, O=mbed TLS, CN=mbed TLS Test intermediate CA 3"

Finally, other
 CAs for specific purposes:
- enco-ca-prstr.pem: has its CN encoded as a printable string, but child cert
 enco-cert-utf8str.pem has its issuer's CN encoded as a UTF-8 string.
- test-ca-v1.crt: v1 "CA", signs
  server1-v1.crt: v1 "intermediate CA", signs

server2-v1*.crt: EE cert (without of with chain in same file)
- keyUsage.decipherOnly.crt: has the decipherOnly keyUsage bit set

End-entity certificates

Short information fields:

- name or pattern
- issuing CA: 1 -> test-ca.crt
2 -> test-ca2.crt
I1 -> test-int-ca.crt
I2 -> test-int-ca2.crt
I3 -> test-int-ca3.crt
O -> other
- key type: R -> RSA, E -> EC
- C -> there is a CRL revoking this cert (see below)
- L -> CN=localhost (useful for local test servers)
- P1, P2 if the file includes parent (resp. parent + grandparent)
- free-form comments

List of certificates:

- cert_example_multi*.crt: 1/O R: subjectAltName
-
cert_example_wildcard.crt: 1 R: wildcard in subject's CN
- cert_md*.crt, cert_sha*.crt: 1 R: signature hash
- cert_v1_with_ext.crt: 1 R: v1 with extensions (illegal)
- cli2.crt: 2 E: basic
- cli-rsa.key, cli-rsa-*.crt: RSA key used for test clients, signed by
the RSA test CA.
- enco-cert-utf8str.pem: see enco-ca-prstr.pem above
- server1*.crt: 1* R C* P1*: misc *(server1-v1 see test-ca-v1.crt above)
*CRL for: .cert_type.crt, .crt, .key_usage.crt, .v1.crt
P1 only for _ca.crt
- server2-v1*.crt: O R: see test-ca-v1.crt above
- server2*.crt: 1 R L: misc
- server3.crt: 1 E L: EC cert signed by RSA CA
- server4.crt: 2 R L: RSA cert signed by EC CA
- server5*.crt: 2* E L: misc *(except server5-selfsigned)
-sha*: hashes
-eku*: extendeKeyUsage (cli/srv = www client/server, cs = codesign, etc)
-ku*: keyUsage (ds = signatures, ke/ka = key exchange/agreement)
- server6-ss-child.crt: O E: "child" of non-CA server5-selfsigned
- server6.crt, server6.pem: 2 E L C: revoked
-
server7*.crt: I1 E L P1*: EC signed by RSA signed by EC
*P1 except 7.crt, P2 _int-ca_ca2.crt

*_space: with PEM error(s)
- server8*.crt: I2 R L: RSA signed by EC signed by RSA (P1 for _int-ca2)
- server9*.crt: 1 R C* L P1*: signed using RSASSA-PSS
*CRL for: 9.crt, -badsign, -with-ca (P1)
- server10*.crt: I3 E L P2/P3

Certificate revocation lists

Signing CA in parentheses (same meaning as certificates).

- crl-ec-sha*.pem: (2) server6.crt
- crl-future.pem: (2) server6.crt + unknown
- crl-rsa-pss-*.pem: (1) server9{,badsign,with-ca}.crt + cert_sha384.crt + unknown
- crl.pem, crl_expired.pem: (1) server1{,.cert_type,.key_usage,.v1}.crt + unknown
- crl_md*.pem: crl_sha*.pem: (1) same as crl.pem
- crt_cat_*.pem: (1+2) concatenations in various orders:
ec = crl-ec-sha256.pem, ecfut = crl-future.pem
rsa = crl.pem, rsabadpem = same with pem error, rsaexp = crl_expired.pem

Note: crl_future would revoke server9 and cert_sha384.crt if signed
by CA 1
crl-rsa-pss* would revoke server6.crt if signed by CA 2

Generation

Newer test files have been generated through commands in the Makefile. The
resulting files are committed to the repository so that the tests can
run without having to re-do the generation and so that the output is the
same for everyone (the generation process is randomized).

The origin of older certificates has not been recorded.
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 9 (0x9)
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=NL, O=PolarSSL, CN=PolarSSL Test CA
Validity
Not Before: Feb 12 14:44:07 2011 GMT
Not After : Feb 12 14:44:07 2021 GMT
Subject: C=NL, O=PolarSSL, CN=PolarSSL Cert SHA256
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit):
00:b9:3c:4a:c5:c8:a3:8e:90:17:a4:9e:52:aa:71:

75:26:61:80:e7:c7:b5:6d:8c:ff:aa:b6:41:26:b7:
be:11:ad:5c:73:16:0c:64:11:48:04:ff:d6:e1:3b:
05:db:89:bb:b3:97:09:d5:1c:14:dd:68:87:39:b0:
3d:71:cb:e2:76:d0:1a:d8:18:2d:80:1b:54:f6:e5:
44:9a:f1:cb:af:61:2e:df:49:0d:9d:09:b7:ed:b1:
fd:3c:fd:3c:fa:24:cf:5d:bf:7c:e4:53:e7:25:b5:
ea:44:22:e9:26:d3:ea:20:94:9e:e6:61:67:ba:2e:
07:67:0b:03:2f:a2:09:ed:f0:33:8f:0b:ce:10:ef:
67:a4:c6:08:da:c1:ed:c2:3f:d7:4a:dd:15:3d:f9:
5e:1c:81:60:46:3e:b5:b3:3d:2f:a6:de:47:1c:bc:
92:ae:eb:df:27:6b:16:56:b7:dc:ec:d1:55:57:a5:
6e:ec:75:25:f5:b7:7b:df:ab:d2:3a:5a:91:98:7d:
97:17:0b:13:0a:a7:6b:4a:8b:c1:47:30:fb:3a:f8:
41:04:d5:c1:df:b8:1d:bf:7b:01:a5:65:a2:e0:1e:
36:b7:a6:5c:cc:30:5a:f8:cd:6f:cd:f1:19:62:25:
ca:01:e3:35:7f:fa:20:f5:dc:fd:69:b2:6a:00:7d:
17:f7
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
X509v3 Subject Key Identifier:
7D:E4:9C:6B:E6:F9:71:7D:46:D2:12:3D:AD:6B:1D:FD:C2:AA:78:4C
X509v3 Authority Key Identifier:
keyid:B4:5A:E4:A5:B3:DE:D2:52:F6:B9:D5:A6:95:0F:EB:3E:BC:C7:FD:FF

Signature Algorithm: sha256WithRSAEncryption
69:ce:f9:a9:d5:e2:32:db:fe:a9:f9:92:7a:d6:76:37:05:51:
c9:e3:a1:03:72:b2:bc:2c:86:4b:31:16:02:10:e8:43:d4:c0:
33:3c:4f:ea:9d:12:6b:57:51:bc:d7:d9:42:56:cf:c7:29:e7:
d7:52:24:49:29:ac:9c:de:8f:cc:ab:1a:a9:62:07:5a:6b:f7:
fb:19:ab:f5:b1:2c:a4:aa:dc:5d:03:73:17:7c:ea:52:44:80:
ca:70:d3:10:c5:2e:fd:9f:d2:0d:65:c4:f2:cc:ef:1b:18:e1:
0a:08:4e:67:d0:56:7f:24:54:2e:73:31:b5:4d:22:74:f8:30:
f9:92:c4:64:c9:46:80:d4:e1:bd:d6:e7:26:ea:bb:c4:fe:6f:
a2:c5:10:e4:64:2f:b0:44:04:2c:b3:44:39:cf:b4:de:ac:83:
43:5e:0b:ca:cd:fb:4e:18:e6:38:39:e7:10:3f:d6:59:17:e7:
42:ef:00:e3:88:c6:43:bc:21:12:bf:20:a8:64:c6:30:dc:8c:
6b:b8:6a:ce:6b:8a:22:3b:d8:af:0c:b4:bb:4d:be:96:dd:40:
d9:87:3e:95:2e:1a:27:23:62:e8:6e:bd:e0:89:d0:a7:28:16:
95:ea:cb:89:a3:f7:7f:fb:0f:ac:ab:d6:a8:b4:cb:43:92:d9:
cb:3e:8a:11
-----BEGIN
CERTIFICATE-----
MIIDQjCCAiqgAwIBAgIBCTANBgkqhkiG9w0BAQsFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTEwMjEyMTQ0NDA3WhcNMjEwMjEyMTQ0NDA3WjA/MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxHTAbBgNVBAMTFFBvbGFyU1NMIENlcnQgU0hBMjU2MIIB

IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuTxKxcijjpAXpJ5SqnF1JmGA
58e1bYz/qrZBJre+Ea1ccxYMZBFIBP/W4TsF24m7s5cJ1RwU3WiHObA9ccvidtAa
2BgtgBtU9uVEmvHLr2Eu30kNnQm37bH9PP08+iTPXb985FPnJbXqRCLpJtPqIJSe
5mFnui4HZwsDL6IJ7fAzjwvOEO9npMYI2sHtwj/XSt0VPfleHIFgRj61sz0vpt5H
HLySruvfJ2sWVrfc7NFVV6Vu7HUl9bd736vSOlqRmH2XFwsTCqdrSovBRzD7OvhB
BNXB37gdv3sBpWWi4B42t6ZczDBa+M1vzfEZYiXKAeM1f/og9dz9abJqAH0X9wID
AQABo00wSzAJBgNVHRMEAjAAMB0GA1UdDgQWBBR95Jxr5vlxfUbSEj2tax39wqp4
TDAfBgNVHSMEGDAWgBS0WuSls97SUva51aaVD+s+vMf9/zANBgkqhkiG9w0BAQsF
AAOCAQEAac75qdXiMtv+qfmSetZ2NwVRyeOhA3KyvCyGSzEWAhDoQ9TAMzxP6p0S
a1dRvNfZQlbPxynn11IkSSmsnN6PzKsaqWIHWmv3+xmr9bEspKrcXQNzF3zqUkSA
ynDTEMUu/Z/SDWXE8szvGxjhCghOZ9BWfyRULnMxtU0idPgw+ZLEZMlGgNThvdbn
Juq7xP5vosUQ5GQvsEQELLNEOc+03qyDQ14Lys37ThjmODnnED/WWRfnQu8A44jG
Q7whEr8gqGTGMNyMa7hqzmuKIjvYrwy0u02+lt1A2Yc+lS4aJyNi6G694InQpygW
lerLiaP3f/sPrKvWqLTLQ5LZyz6KEQ==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB3jCCAYWgAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDAwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQznn9zHHwL
GO8VR4W9V7vMlxCdoojzEOiX5Y6JtPtFOz866ueHY6zoN0/mJ6DnqnSXilJIUUeW
6eGfqmka7nxko4GRMIGOMB0GA1UdDgQWBBSh3uHkX5nj86yFEFwjscSWM40P+jBf
BgNVHSMEWDBWgBQlFYvU5WboI4fcdPoiQs8/fPHZraEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggkA/KCWhcqToHAw
DAYDVR0TBAUwAwEB/zAKBggqhkjOPQQDAgNHADBEAiBasbuinP+pJTU4oDCVD8zQ
1rJBDSOKIEyWu84/D6Hj6wIgVMPUoO01bPhzllAa/gW8Xk/daey09SBgN3AT9pWU
TDA=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIBpTCCAUugAwIBAgIJAPygloXKk6BwMAoGCCqGSM49BAMCMC8xCzAJBgNVBAYT
AlVLMREwDwYDVQQKDAhtYmVkIFRMUzENMAsGA1UEAwwEQ0EwMDAeFw0xNzA2MjIx
MTUwMzJaFw0yNzA2MjMxMTUwMzJaMC8xCzAJBgNVBAYTAlVLMREwDwYDVQQKDAht
YmVkIFRMUzENMAsGA1UEAwwEQ0EwMDBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IA
BFW41/qAwAPpy+Txdc7PKmzZsq9CPiujKU4vpF1ekXnGx2HP420QobwBVVWhkzRm
LwdboH2j65dcCKjQ7mv/dxKjUDBOMB0GA1UdDgQWBBQlFYvU5WboI4fcdPoiQs8/
fPHZrTAfBgNVHSMEGDAWgBQlFYvU5WboI4fcdPoiQs8/fPHZrTAMBgNVHRMEBTAD
AQH/MAoGCCqGSM49BAMCA0gAMEUCIQC7iRcVzwMyfVK5imirJ7MqJQ04euH4CLOt
IZ+SNfaERAIgSU0MWFDosVEIpg8YMqIHeF7Mg4ZyH6+fGazJgVLttUY=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTkwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMjAwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATGebrN8JxE
heOdCxD+mhnQ4zMUxF1WUkmAAHIUw089BYiH9SAwYS/M5tnl+R8fbjvoGqSpR6Tk
V9EU3CQyIoxwo4GJMIGGMB0GA1UdDgQWBBTZs6oChL1c2CSZXY2YFQkkqg+lzDBX

BgNVHSMEUDBOgBRQMc94kTqW+zQO3lo2WMI/81k3c6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTE4ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgRVGZReXKvdMHhwLbPvbrTVLeAGDqmqMH
/WqD4u23QBgCID/QtFaiawjviNFEdtU7JK6v4ZY0PQ0a0+HLZIHLi9ah
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTgwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTkwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQJyRCHND78
KxZHoHHdOTjPuD6HjHPnEKX8apblUpETDJuLW7YR3V8Q0dTac+JHiR6e2l4DlDbf
5bTiyFoAzw9yo4GJMIGGMB0GA1UdDgQWBBRQMc94kTqW+zQO3lo2WMI/81k3czBX
BgNVHSMEUDBOgBSDbIpYntlhJ0GgIsyd75XRhlC18qEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTE3ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgIzGOZqJRmvygzvLm8zxZFyoNpcT7e26H
nZd5xFIzEakCIHGYcUXzt+owSVlLmrlW8gQcB81ErQbxuBTAsvpaaKSS
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTcwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTgwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASsc/JkNcYf
bMgpOfrL5kKOGxOJaGS6SQIeNO33UeBpToe1bU2acN652xjvcGo0fJEtxg2fcPHR
hTnGMBD1u1N2o4GJMIGGMB0GA1UdDgQWBBSDbIpYntlhJ0GgIsyd75XRhlC18jBX
BgNVHSMEUDBOgBSnjWvpWxZcFnfQ2KGtCg/u6fT/D6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTE2ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAJo2NXfJU1sK6SVTu4OV21FKITlXntMi
oenYMsBjzO8oAiEAidSELcLjjAHi3mfBARvCgKlRhmbNEMCHQT7Ha7ZQoRw=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTYwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTcwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAARrISq2zO9m
D29YCLHB56FdU/RINtRhfeLtM+u5o3HaAnopy0S98RzuEGELjpzr8ZI6kkMMZsj8
nFZQF8HfuE0go4GJMIGGMB0GA1UdDgQWBBSnjWvpWxZcFnfQ2KGtCg/u6fT/DzBX
BgNVHSMEUDBOgBRTw3K0Psy3u/6+3KKSoaQqJnPvPqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTE1ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgDgXjoc6FfMF5W0NziV6vx2BOPNWav01Z
ynEP4h9ULnUCIQC1rU4sEId3UdjzTKhpSGTKtaOuPG+b0YdEMPimI4jmVw==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTUwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTYwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQ7Vsp7JmDN

kgPh/+zmIPkd7o0xot/WPMFn3uAsGtsU385MF0fmhfFLhRbbH9h4JjYHj8y0spU3
buUXhftvAZVbo4GJMIGGMB0GA1UdDgQWBBRTw3K0Psy3u/6+3KKSoaQqJnPvPjBX
BgNVHSMEUDBOgBR1mXlrdW5rx1VnqMMnUBXo0WWGWqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTE0ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAMJnGjE9v3SjuGfi0jNByrwyNfhlTHMh
FhPQidNrDpXwAiEAqYtNiV8t9RrAa9GC6FWDuJpvIiU6FsE+lFq6uIq/J2E=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTQwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTUwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQlKUiMoSss
/hsTasedqdB2BCOGJhTt0hgUGeUnWNZ1svO4yn0GkFHZ08++fl2MKqjpj+VXq0JS
FFyGUOgmgi3Ho4GJMIGGMB0GA1UdDgQWBBR1mXlrdW5rx1VnqMMnUBXo0WWGWjBX
BgNVHSMEUDBOgBRNsJB++ccSBmbCCKBxi4CjXROBk6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTEzggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAKYOIo+fdCQRqpH4LN8qUK1aKzKmWGxS
fGzEEkg/29bMAiAl95cmucoCDMq2Ab8Coc0dEqyJ6+rAPMLBCbGawyiW6A==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTMwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTQwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATRMZN0RHzP
donNmZuq9XPhzvQ52TaokxT39qpQtlFyvUuEGKrLoNvdcpARaA0rGput6RLAQOVU
iNVlJ3Ipj789o4GJMIGGMB0GA1UdDgQWBBRNsJB++ccSBmbCCKBxi4CjXROBkzBX
BgNVHSMEUDBOgBTmVnUSF2MYwws/nCMv7b1wJVkDmqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTEyggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgVfuLpjp08AaxKWf6cuZUUCRd7CojSS1I
71hzeUyFS+sCIQDNJI6P/pBbiHgTaGlBAgfcEfmxmbY0n4xZndtxIkmyVA==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTIwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTMwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATrkzCJLznh
lhnsv1RXB9kfeaD+cIruPQ0cItBDGpdvD8xbBVvQci4+RG2RVUCSWRhkFYjSsUSM
0QHMQnBFlhw2o4GJMIGGMB0GA1UdDgQWBBTmVnUSF2MYwws/nCMv7b1wJVkDmjBX
BgNVHSMEUDBOgBTZTtbi+j0Sm/Zs/+gTkWdASpQzfqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTExggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgWsm+rHJgwUEyNm8EKbEds5yurpp5/3y5
PsvXJVDqxogCIQDUP0Jcl3A907CE2tPVXSgD6LQ6CPu19mixemPw60yijA==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G

A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTEwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTIwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATDE9LPlLPc
gZ3b0BchR/AkhNEP9HAavwYadJIyzoPo5edCVnboQH786jsZwZNZoC0gHDAhCmGc
IfRenISAoVuPo4GJMIGGMB0GA1UdDgQWBBTZTtbi+j0Sm/Zs/+gTkWdASpQzfjBX
BgNVHSMEUDBOgBSOSt6ePyMRT6PGMaIi7FqNX9MKtKEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTEwggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgYYF5AnRV7eh2hLD5Dz//pceMTKz9Ls46
E6DxvbfDHikCIFttlGrOCZVyS4ocsjuKIELVUX5qfygI0sn4kU3qCTs2
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTAwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATZwR+WK6NB
F/7riFdN63c8hjYddZRR4lrzVNPwiBQxnnxwpPyrD9A6aPPmLc6SqGOJW4ZGVCco
IBze9RJVeiB9o4GJMIGGMB0GA1UdDgQWBBSOSt6ePyMRT6PGMaIi7FqNX9MKtDBX
BgNVHSMEUDBOgBQtxZSLJAkEz+2RKMQexM6EtsfgcqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA5ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgN//NqM0FrkrMjmxoeCY9DgxkH2R6sQ4d
NgtwCZAIqEICIBs4vupaVcuvni9tltbP26wi7c0FR+blZuo5DPIA3SVe
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDkwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTAwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAR6jlGKbJd5
hiDxN789gkOcwpyHI9wRwCrADAOwOkMePBPRlwGdm7mw7Z/EAmu26zRm/hcyrs4M
qk2LabDjPI9Xo4GJMIGGMB0GA1UdDgQWBBQtxZSLJAkEz+2RKMQexM6EtsfgcjBX
BgNVHSMEUDBOgBT6gyXHzPIPYc1Vr1aGiLLeMh4HpqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA4ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgP7S8vFstfUBdNe6ym5GYG5Q+aBVEKqRs
fVW7HNUktSYCIQDo6Jua6o/DJbrpq4qYWq5gv4yGyzPTN+3IaKrEICdaaw==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDgwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDkwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAR7ZB16+t6E
sfahGyKUGJW5mezkzjdaYvc4lbJaKNRwFRfc3F/fmNOSsUFSg/F0N+vUE+doKiPC
8wRwLzvm4s+5o4GJMIGGMB0GA1UdDgQWBBT6gyXHzPIPYc1Vr1aGiLLeMh4HpjBX
BgNVHSMEUDBOgBS40mLt93U8Sh8ZGiDVAhRSiBPcXqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA3ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgO4el1ZPhlIli/qNR2SIEiuvs5Mmy868i
N2Rv5X/VxIECIA/8rUALQxW38XSdBVX3e/jzu7ju47n1YwEqD9K9WdVv
-----END

CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDcwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDgwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAARpQeQ/YGQj
nl7Szo6WStJ1u7xunTL5jBkXH8aAVSm0qiX4AD/7YPxa5EnGzZdLTn25vQVnfQAG
pMx8P1lYiGYCo4GJMIGGMB0GA1UdDgQWBBS40mLt93U8Sh8ZGiDVAhRSiBPcXjBX
BgNVHSMEUDBOgBREq5J3toJPxZ3O+ssJ5vkkU0RJE6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA2ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhANwGf+F4a+kmXWz8UjSpRkaToTV6EFWw
/Tjzj0tQhDoAAiEA19RxeWOVBBpM6LOHg6v5Lf54YN1snkLf+sEXyZCuWQQ=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDYwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDcwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASNOj4d4MEA
7p/3miijqG4ToE4opKPAm+3BTIGrJTYT14++TSiUICl0ASXj+xeUcLMIaXTN042s
LsHxpShzQaL0o4GJMIGGMB0GA1UdDgQWBBREq5J3toJPxZ3O+ssJ5vkkU0RJEzBX
BgNVHSMEUDBOgBSjovYaC/m6Li9Tp0V9iZRs9267Q6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA1ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAKGcf+c442c/XiwubbaiQvsoZ7EoVxuM
oKmia0gPyBNkAiEA83asjJ5FDXQuLyZpczviXrbmqgCPOfYadtvkc0cxMis=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDUwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDYwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASA9qWoAUHr
nn+3kxyNrjPJk82WDLimW21RN51uxpobadv8YgGEDRdP+Ok+uRqQSUsA6ZXfF3iG
r2GjfQ3wMDH8o4GJMIGGMB0GA1UdDgQWBBSjovYaC/m6Li9Tp0V9iZRs9267QzBX
BgNVHSMEUDBOgBTXh06MAV9S4l4lG1TKOrKRBh4qn6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA0ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgcjZNFWJtlDmoPZbAxqsGczRYK0lfPgu6
g1H7pp0ce+wCIDj9BRZM2OB9EF0e+MDKGjyZGfvfrL6Ir47x/KrM6H8T
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDQwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDUwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQEdT0OFf5G
UcrgX2XllCyJzP94NZ464GsgB6psNLsDeL+j7AU+oJy7VLvW/lHh3ODgl08Z9bhq
LFBmNjnHbm8Qo4GJMIGGMB0GA1UdDgQWBBTXh06MAV9S4l4lG1TKOrKRBh4qnzBX
BgNVHSMEUDBOgBQox4F1NsZunlsduoGvzIgRSYfB36EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAzggEBMAwGA1UdEwQF

MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAIW++zqDZlLLUk/emePohdNOp5JO3wS9
XvkBJ6Wua7GBAiAdx+EKmdjVrwnzrQltTgnmSfGMXhKNYifK3uD83W3pcQ==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDMwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDQwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQUXDgcUVNT
9hovbZE5HL6rjOb7C55wEuWKThV/CcZ4rWrXx7VXHYdD/R3aDA7JSvYpm2sTok4i
sblDzhZM/GDNo4GJMIGGMB0GA1UdDgQWBBQox4F1NsZunlsduoGvzIgRSYfB3zBX
BgNVHSMEUDBOgBQApzZdtBdD3dLxouQpr/aDiVttd6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAyggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgAkiNhqFAZXSUWEDK91OZvQGdeZOtd6mC
+Wv3fGk3t28CIEKOwidkUTUaiPdZ4efmAr+CEeGzdq27ob2S+nqqHqgV
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDIwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDMwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQRDXDNIi1p
ereudhqwa2LslXgsxnB63Hu5y5lg+1WPruIYPzD/Ho0APveVdzFLVji19+bE4+tF
PYL1SpsN1WfWo4GJMIGGMB0GA1UdDgQWBBQApzZdtBdD3dLxouQpr/aDiVttdzBX
BgNVHSMEUDBOgBT5RCgQ0AlZTQbfFB2+6+w0XRvydaEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAxggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAOnd+7bAofkHVa4KFNjv3TCegw1lrhuM
8Of8wgvrTEGoAiEAsS8iKMpSfXH4D0egg4gLamE6akde965rDtySU+ve9lg=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDEwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDIwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQWHpv1i6lf
wvNPOP5ka6S0n55EvzoaYK6pbTXP6yMOW/4XZSPKx5Zoq4FMe0cKzGIIFL1rzj1V
2czYB+qvLhyio4GJMIGGMB0GA1UdDgQWBBT5RCgQ0AlZTQbfFB2+6+w0XRvydTBX
BgNVHSMEUDBOgBSh3uHkX5nj86yFEFwjscSWM40P+qEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAI7unGW/gr9tOc3i+dF5N815srgh+FrX
oj9Et74EcSpTAiBubv+vOH0DE0gmYI11HeAIgutWqqMIC72dZlwTF/Vi3g==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB3jCCAYWgAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDAwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQznn9zHHwL
GO8VR4W9V7vMlxCdoojzEOiX5Y6JtPtFOz866ueHY6zoN0/mJ6DnqnSXilJIUUeW

6eGfqmka7nxko4GRMIGOMB0GA1UdDgQWBBSh3uHkX5nj86yFEFwjscSWM40P+jBf
BgNVHSMEWDBWgBQlFYvU5WboI4fcdPoiQs8/fPHZraEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggkA/KCWhcqToHAw
DAYDVR0TBAUwAwEB/zAKBggqhkjOPQQDAgNHADBEAiBasbuinP+pJTU4oDCVD8zQ
1rJBDSOKIEyWu84/D6Hj6wIgVMPUoO01bPhzllAa/gW8Xk/daey09SBgN3AT9pWU
TDA=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIBpTCCAUugAwIBAgIJAPygloXKk6BwMAoGCCqGSM49BAMCMC8xCzAJBgNVBAYT
AlVLMREwDwYDVQQKDAhtYmVkIFRMUzENMAsGA1UEAwwEQ0EwMDAeFw0xNzA2MjIx
MTUwMzJaFw0yNzA2MjMxMTUwMzJaMC8xCzAJBgNVBAYTAlVLMREwDwYDVQQKDAht
YmVkIFRMUzENMAsGA1UEAwwEQ0EwMDBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IA
BFW41/qAwAPpy+Txdc7PKmzZsq9CPiujKU4vpF1ekXnGx2HP420QobwBVVWhkzRm
LwdboH2j65dcCKjQ7mv/dxKjUDBOMB0GA1UdDgQWBBQlFYvU5WboI4fcdPoiQs8/
fPHZrTAfBgNVHSMEGDAWgBQlFYvU5WboI4fcdPoiQs8/fPHZrTAMBgNVHRMEBTAD
AQH/MAoGCCqGSM49BAMCA0gAMEUCIQC7iRcVzwMyfVK5imirJ7MqJQ04euH4CLOt
IZ+SNfaERAIgSU0MWFDosVEIpg8YMqIHeF7Mg4ZyH6+fGazJgVLttUY=
-----END
CERTIFICATE-----
Certificate Request check Server1 SHA1
depends_on:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_csr_check:"data_files/server1.key":"data_files/server1.req.sha1":MBEDTLS_MD_SHA1:0:0

Certificate Request check Server1 SHA224
depends_on:MBEDTLS_SHA256_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_csr_check:"data_files/server1.key":"data_files/server1.req.sha224":MBEDTLS_MD_SHA224:0:0

Certificate Request check Server1 SHA256
depends_on:MBEDTLS_SHA256_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_csr_check:"data_files/server1.key":"data_files/server1.req.sha256":MBEDTLS_MD_SHA256:0:0

Certificate Request check Server1 SHA384
depends_on:MBEDTLS_SHA512_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_csr_check:"data_files/server1.key":"data_files/server1.req.sha384":MBEDTLS_MD_SHA384:0:0

Certificate Request check Server1 SHA512
depends_on:MBEDTLS_SHA512_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_csr_check:"data_files/server1.key":"data_files/server1.req.sha512":MBEDTLS_MD_SHA512:0:0

Certificate Request check Server1
MD4
depends_on:MBEDTLS_MD4_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_csr_check:"data_files/server1.key":"data_files/server1.req.md4":MBEDTLS_MD_MD4:0:0

Certificate Request check Server1 MD5
depends_on:MBEDTLS_MD5_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_csr_check:"data_files/server1.key":"data_files/server1.req.md5":MBEDTLS_MD_MD5:0:0

Certificate Request check Server1 key_usage
depends_on:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_csr_check:"data_files/server1.key":"data_files/server1.req.key_usage":MBEDTLS_MD_SHA1:MBEDTLS_X509_KU_DIGITAL_SIGNATURE | MBEDTLS_X509_KU_NON_REPUDIATION | MBEDTLS_X509_KU_KEY_ENCIPHERMENT:0

Certificate Request check Server1 ns_cert_type
depends_on:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_csr_check:"data_files/server1.key":"data_files/server1.req.cert_type":MBEDTLS_MD_SHA1:0:MBEDTLS_X509_NS_CERT_TYPE_SSL_SERVER

Certificate Request check Server1 key_usage + ns_cert_type
depends_on:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15
x509_csr_check:"data_files/server1.key":"data_files/server1.req.ku-ct":MBEDTLS_MD_SHA1:MBEDTLS_X509_KU_DIGITAL_SIGNATURE
| MBEDTLS_X509_KU_NON_REPUDIATION | MBEDTLS_X509_KU_KEY_ENCIPHERMENT:MBEDTLS_X509_NS_CERT_TYPE_SSL_SERVER

Certificate Request check Server5 ECDSA, key_usage
depends_on:MBEDTLS_SHA1_C:MBEDTLS_ECDSA_C:MBEDTLS_ECDSA_DETERMINISTIC:MBEDTLS_ECP_DP_SECP256R1_ENABLED
x509_csr_check:"data_files/server5.key":"data_files/server5.req.ku.sha1":MBEDTLS_MD_SHA1:MBEDTLS_X509_KU_DIGITAL_SIGNATURE | MBEDTLS_X509_KU_NON_REPUDIATION:0

Certificate write check Server1 SHA1
depends_on:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_MD5_C
x509_crt_check:"data_files/server1.key":"":"C=NL,O=PolarSSL,CN=PolarSSL Server 1":"data_files/test-ca.key":"PolarSSLTest":"C=NL,O=PolarSSL,CN=PolarSSL Test CA":"1":"20110212144406":"20210212144406":MBEDTLS_MD_SHA1:0:0:-1:"data_files/server1.crt"

Certificate write check Server1 SHA1, key_usage
depends_on:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_MD5_C
x509_crt_check:"data_files/server1.key":"":"C=NL,O=PolarSSL,CN=PolarSSL Server 1":"data_files/test-ca.key":"PolarSSLTest":"C=NL,O=PolarSSL,CN=PolarSSL Test CA":"1":"20110212144406":"20210212144406":MBEDTLS_MD_SHA1:MBEDTLS_X509_KU_DIGITAL_SIGNATURE | MBEDTLS_X509_KU_NON_REPUDIATION | MBEDTLS_X509_KU_KEY_ENCIPHERMENT:0:-1:"data_files/server1.key_usage.crt"

Certificate write check Server1 SHA1, ns_cert_type
depends_on:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_MD5_C
x509_crt_check:"data_files/server1.key":"":"C=NL,O=PolarSSL,CN=PolarSSL Server 1":"data_files/test-ca.key":"PolarSSLTest":"C=NL,O=PolarSSL,CN=PolarSSL Test CA":"1":"20110212144406":"20210212144406":MBEDTLS_MD_SHA1:0:MBEDTLS_X509_NS_CERT_TYPE_SSL_SERVER:-1:"data_files/server1.cert_type.crt"

Certificate write check Server1 SHA1, version 1
depends_on:MBEDTLS_SHA1_C:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_MD5_C
x509_crt_check:"data_files/server1.key":"":"C=NL,O=PolarSSL,CN=PolarSSL Server 1":"data_files/test-ca.key":"PolarSSLTest":"C=NL,O=PolarSSL,CN=PolarSSL Test CA":"1":"20110212144406":"20210212144406":MBEDTLS_MD_SHA1:0:0:MBEDTLS_X509_CRT_VERSION_1:"data_files/server1.v1.crt"

X509 String to Names #1
mbedtls_x509_string_to_names:"C=NL,O=Offspark\, Inc., OU=PolarSSL":"C=NL, O=Offspark, Inc., OU=PolarSSL":0

X509 String to Names #2
mbedtls_x509_string_to_names:"C=NL, O=Offspark, Inc., OU=PolarSSL":"":MBEDTLS_ERR_X509_UNKNOWN_OID

X509 String to Names #3 (Name precisely 255 bytes)
mbedtls_x509_string_to_names:"C=NL,
O=123456789012345,OU=PolarSSL":"C=NL,
O=123456789012345,
OU=PolarSSL":0

X509 String to Names #4 (Name larger than 255 bytes)
mbedtls_x509_string_to_names:"C=NL,
O=1234567890123456,
OU=PolarSSL":"":MBEDTLS_ERR_X509_INVALID_NAME

X509 String to Names #5 (Escape non-allowed characters)
mbedtls_x509_string_to_names:"C=NL, O=Offspark\a Inc., OU=PolarSSL":"":MBEDTLS_ERR_X509_INVALID_NAME

X509 String to Names #6 (Escape at end)
mbedtls_x509_string_to_names:"C=NL, O=Offspark\":"":MBEDTLS_ERR_X509_INVALID_NAME
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAqQIfPUBq1VVTi/027oJlLhVhXom/uOhFkNvuiBZS0/FDUEeW
Ellkh2v9K+BG+XO+3c+S4ZFb7Wagb4kpeUWA0INq1UFDd185fAkER4KwVzlw7aPs
FRkeqDMIR8EFQqn9TMO0390GH00QUUBncxMPQPhtgSVfCrFTxjB+FTms+Vruf5Ke
pgVb5xOXhbUjktnUJAbVCSWJdQfdphqPPwkZvq1lLGTrlZvc/kFeF6babFtpzAK6
FCwWJJxK3M3Q91Jnc/EtoCP9fvQxyi1wyokLBNsupk9wbp7OvViJ4lNZnm5akmXi
iD8MlBmj3eXonZUT7Snbq3AS3FrKaxerUoJUsQIDAQABAoIBABaJ9eiRQq4Ypv+w
UTcVpLC0oTueWzcpor1i1zjG4Vzqe/Ok2FqyGToGKMlFK7Hwwa+LEyeJ3xyV5yd4
v1Mw9bDZFdJC1eCBjoUAHtX6k9HOE0Vd6woVQ4Vi6OPI1g7B5Mnr/58rNrnN6TMs

x58NF6euecwTU811QJrZtLbX7j2Cr28yB2Vs8qyYlHwVw5jbDOv43D7vU5gmlIDN
0JQRuWAnOuPzZNoJr4SfJKqHNGxYYY6pHZ1s0dOTLIDb/B8KQWapA2kRmZyid2EH
nwzgLbAsHJCf+bQnhXjXuxtUsrcIL8noZLazlOMxwNEammglVWW23Ud/QRnFgJg5
UgcAcRECgYEA19uYetht5qmwdJ+12oC6zeO+vXLcyD9gon23T5J6w2YThld7/OW0
oArQJGgkAdaq0pcTyOIjtTQVMFygdVmCEJmxh/3RutPcTeydqW9fphKDMej32J8e
GniGmNGiclbcfNOS8E5TGp445yZb9P1+7AHng16bGg3Ykj5EA4G+HCcCgYEAyHAl
//ekk8YjQElm+8izLtFkymIK0aCtEe9C/RIRhFYBeFaotC5dStNhBOncn4ovMAPD
lX/92yDi9OP8PPLN3a4B9XpW3k/SS5GrbT5cwOivBHNllZSmu/2qz5WPGcjVCOrB
LYl3YWr2h3EGKICT03kEoTkiDBvCeOpW7cCGl2cCgYBD5whoXHz1+ptPlI4YVjZt
Xh86aU+ajpVPiEyJ84I6xXmO4SZXv8q6LaycR0ZMbcL+zBelMb4Z2nBv7jNrtuR7
ZF28cdPv+YVr3esaybZE/73VjXup4SQPH6r3l7qKTVi+y6+FeJ4b2Xn8/MwgnT23
8EFrye7wmzpthrjOgZnUMQKBgE9Lhsz/5J0Nis6Y+2Pqn3CLKEukg9EwtqdctZy0
5Dcta0F3TyCRIxlCDKTL/BslqMtfAdY4H268UO0+8IAQMn9boqzBrHIgs/pvc5kx
TbKHmw2wtWR6vYersBKVgVpbCGSRssDYHGFu1n74qM4HJ/RGcR1zI9QUe1gopSFD
xDtLAoGAVAdWvrqDwgoL2hHW3scGpxdE/ygJDOwHnf+1B9goKAOP5lf2FJaiAxf3
ectoPOgZbCmm/iiDmigu703ld3O+VoCLDD4qx3R+KyALL78gtVJYzSRiKhzgCZ3g
mKsIVRBq4IfwiwyMNG2BYZQAwbSDjjPtn/kPBduPzPj7eriByhI=
-----END
RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIICUjCCAdegAwIBAgIJAMFD4n5iQ8zoMAoGCCqGSM49BAMCMD4xCzAJBgNVBAYT
Ak5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBF
QyBDQTAeFw0xMzA5MjQxNTQ5NDhaFw0yMzA5MjIxNTQ5NDhaMD4xCzAJBgNVBAYT
Ak5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBF
QyBDQTB2MBAGByqGSM49AgEGBSuBBAAiA2IABMPaKzRBN1gvh1b+/Im6KUNLTuBu
ww5XUzM5WNRStJGVOQsj318XJGJI/BqVKc4sLYfCiFKAr9ZqqyHduNMcbli4yuiy
aY7zQa0pw7RfdadHb9UZKVVpmlM7ILRmFmAzHqOBoDCBnTAdBgNVHQ4EFgQUnW0g
JEkBPyvLeLUZvH4kydv7NnwwbgYDVR0jBGcwZYAUnW0gJEkBPyvLeLUZvH4kydv7
NnyhQqRAMD4xCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UE
AxMTUG9sYXJzc2wgVGVzdCBFQyBDQYIJAMFD4n5iQ8zoMAwGA1UdEwQFMAMBAf8w
CgYIKoZIzj0EAwIDaQAwZgIxAMO0YnNWKJUAfXgSJtJxexn4ipg+kv4znuR50v56
t4d0PCu412mUC6Nnd7izvtE2MgIxAP1nnJQjZ8BWukszFQDG48wxCCyci9qpdSMv
uCjn8pwUOkABXK8Mss90fzCfCEOtIA==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB/TCCAYCgAwIBAgIBATAMBggqhkjOPQQDAgUAMD4xCzAJBgNVBAYTAk5MMREw
DwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBFQyBDQTAe
Fw0wMzA5MjQxNTQ5NDhaFw0xMzA5MjQxNTQ5NDhaMD4xCzAJBgNVBAYTAk5MMREw
DwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBFQyBDQTB2
MBAGByqGSM49AgEGBSuBBAAiA2IABMPaKzRBN1gvh1b+/Im6KUNLTuBuww5XUzM5
WNRStJGVOQsj318XJGJI/BqVKc4sLYfCiFKAr9ZqqyHduNMcbli4yuiyaY7zQa0p
w7RfdadHb9UZKVVpmlM7ILRmFmAzHqNQME4wDAYDVR0TBAUwAwEB/zAdBgNVHQ4E
FgQUnW0gJEkBPyvLeLUZvH4kydv7NnwwHwYDVR0jBBgwFoAUnW0gJEkBPyvLeLUZ
vH4kydv7NnwwDAYIKoZIzj0EAwIFAANpADBmAjEAvQ/49lXXrLYdOIGtTaYWjpZP
tRBXQiGPMzUvmKBk7gM7bF4iFPsdJikyXHmuwv3RAjEA8vtUX8fAAB3fbh5dEXRm
l7tz0Sw/RW6AHFtaIauGkhHqeKIaKIi6WSgHu6x97uyg
-----END

CERTIFICATE-----
MD process
mbedtls_md_process:

MD NULL/uninitialised arguments
md_null_args:

Information on MD2
depends_on:MBEDTLS_MD2_C
md_info:MBEDTLS_MD_MD2:"MD2":16

Information on MD4
depends_on:MBEDTLS_MD4_C
md_info:MBEDTLS_MD_MD4:"MD4":16

Information on MD5
depends_on:MBEDTLS_MD5_C
md_info:MBEDTLS_MD_MD5:"MD5":16

Information on RIPEMD160
depends_on:MBEDTLS_RIPEMD160_C
md_info:MBEDTLS_MD_RIPEMD160:"RIPEMD160":20

Information on SHA1
depends_on:MBEDTLS_SHA1_C
md_info:MBEDTLS_MD_SHA1:"SHA1":20

Information on SHA224
depends_on:MBEDTLS_SHA256_C
md_info:MBEDTLS_MD_SHA224:"SHA224":28

Information on SHA256
depends_on:MBEDTLS_SHA256_C
md_info:MBEDTLS_MD_SHA256:"SHA256":32

Information on SHA384
depends_on:MBEDTLS_SHA512_C
md_info:MBEDTLS_MD_SHA384:"SHA384":48

Information on SHA512
depends_on:MBEDTLS_SHA512_C
md_info:MBEDTLS_MD_SHA512:"SHA512":64

generic mbedtls_md2 Test vector RFC1319 #1
depends_on:MBEDTLS_MD2_C
md_text:"MD2":"":"8350e5a3e24c153df2275c9f80692773"

generic mbedtls_md2 Test vector

RFC1319 #2
depends_on:MBEDTLS_MD2_C
md_text:"MD2":"a":"32ec01ec4a6dac72c0ab96fb34c0b5d1"

generic mbedtls_md2 Test vector RFC1319 #3
depends_on:MBEDTLS_MD2_C
md_text:"MD2":"abc":"da853b0d3f88d99b30283a69e6ded6bb"

generic mbedtls_md2 Test vector RFC1319 #4
depends_on:MBEDTLS_MD2_C
md_text:"MD2":"message digest":"ab4f496bfb2a530b219ff33031fe06b0"

generic mbedtls_md2 Test vector RFC1319 #5
depends_on:MBEDTLS_MD2_C
md_text:"MD2":"abcdefghijklmnopqrstuvwxyz":"4e8ddff3650292ab5a4108c3aa47940b"

generic mbedtls_md2 Test vector RFC1319 #6
depends_on:MBEDTLS_MD2_C
md_text:"MD2":"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789":"da33def2a
42df13975352846c30338cd"

generic mbedtls_md2 Test vector RFC1319 #7
depends_on:MBEDTLS_MD2_C
md_text:"MD2":"12345678901234567890123456789012345678901234567890123456789012345678901234567890
0":"d5976f79d83d3a0dc9806c3c66f3efd8"

generic mbedtls_md4 Test vector RFC1320 #1
depends_on:MBEDTLS_MD4_C
md_text:"MD4":"":"31d6cfe0d16ae931b73c59d7e0c089c0"

generic
mbedtls_md4 Test vector RFC1320 #2
depends_on:MBEDTLS_MD4_C
md_text:"MD4":"a":"bde52cb31de33e46245e05fbdbd6fb24"

generic mbedtls_md4 Test vector RFC1320 #3
depends_on:MBEDTLS_MD4_C
md_text:"MD4":"abc":"a448017aaf21d8525fc10ae87aa6729d"

generic mbedtls_md4 Test vector RFC1320 #4
depends_on:MBEDTLS_MD4_C
md_text:"MD4":"message digest":"d9130a8164549fe818874806e1c7014b"

generic mbedtls_md4 Test vector RFC1320 #5
depends_on:MBEDTLS_MD4_C
md_text:"MD4":"abcdefghijklmnopqrstuvwxyz":"d79e1c308aa5bbcdeea8ed63df412da9"

generic mbedtls_md4 Test vector RFC1320 #6

depends_on:MBEDTLS_MD4_C
md_text:"MD4":"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789":"043f8582f241db351ce627e153e7f0e4"

generic mbedtls_md4 Test vector RFC1320 #7
depends_on:MBEDTLS_MD4_C
md_text:"MD4":"12345678901234567890123456789012345678901234567890123456789012345678901234567890":"e33b4ddc9c38f2199c3e7b164fcc0536"

generic mbedtls_md5 Test vector RFC1321 #1
depends_on:MBEDTLS_MD5_C
md_text:"MD5":"":"d41d8cd98f00b204e9800998ecf8427e"

generic
mbedtls_md5 Test vector RFC1321 #2
depends_on:MBEDTLS_MD5_C
md_text:"MD5":"a":"0cc175b9c0f1b6a831c399e269772661"

generic mbedtls_md5 Test vector RFC1321 #3
depends_on:MBEDTLS_MD5_C
md_text:"MD5":"abc":"900150983cd24fb0d6963f7d28e17f72"

generic mbedtls_md5 Test vector RFC1321 #4
depends_on:MBEDTLS_MD5_C
md_text:"MD5":"message digest":"f96b697d7cb7938d525a2f31aaf161d0"

generic mbedtls_md5 Test vector RFC1321 #5
depends_on:MBEDTLS_MD5_C
md_text:"MD5":"abcdefghijklmnopqrstuvwxyz":"c3fcd3d76192e4007dfb496cca67e13b"

generic mbedtls_md5 Test vector RFC1321 #6
depends_on:MBEDTLS_MD5_C
md_text:"MD5":"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789":"d174ab98d277d9f5a5611c2c9f419d9f"

generic mbedtls_md5 Test vector RFC1321 #7
depends_on:MBEDTLS_MD5_C
md_text:"MD5":"12345678901234567890123456789012345678901234567890123456789012345678901234567890":"57edf4a22be3c955ac49da2e2107b67a"

generic mbedtls_ripemd160 Test vector from paper #1
depends_on:MBEDTLS_RIPEMD160_C
md_text:"RIPEMD160":"":"9c1185a5c5e9fc54612808977ee8f548b2258d31"

generic
mbedtls_ripemd160 Test vector from paper #2
depends_on:MBEDTLS_RIPEMD160_C
md_text:"RIPEMD160":"a":"0bdc9d2d256b3ee9daae347be6f4dc835a467ffe"

generic mbedtls_ripemd160 Test vector from paper #3
depends_on:MBEDTLS_RIPEMD160_C
md_text:"RIPEMD160":"abc":"8eb208f7e05d987a9b044a8e98c6b087f15a0bfc"

generic mbedtls_ripemd160 Test vector from paper #4
depends_on:MBEDTLS_RIPEMD160_C
md_text:"RIPEMD160":"message digest":"5d0689ef49d2fae572b881b123a85ffa21595f36"

generic mbedtls_ripemd160 Test vector from paper #5
depends_on:MBEDTLS_RIPEMD160_C
md_text:"RIPEMD160":"abcdefghijklmnopqrstuvwxyz":"f71c27109c692c1b56bbdceb5b9d2865b3708dbc"

generic mbedtls_ripemd160 Test vector from paper #6
depends_on:MBEDTLS_RIPEMD160_C
md_text:"RIPEMD160":"abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq":"12a053384a9c0c88e405a06c27dcf49ada62eb2b"

generic mbedtls_ripemd160 Test vector from paper #7
depends_on:MBEDTLS_RIPEMD160_C
md_text:"RIPEMD160":"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789":"b0e20b6e3116640286ed3a87a5713079b21f5189"

generic
mbedtls_ripemd160 Test vector from paper #8
depends_on:MBEDTLS_RIPEMD160_C
md_text:"RIPEMD160":"12345678901234567890123456789012345678901234567890123456789012345678901234567890":"9b752e45573d4b39f4dbd3323cab82bf63326bfb"

generic HMAC-MD2 Hash File OpenSSL test #1
depends_on:MBEDTLS_MD2_C
mbedtls_md_hmac:"MD2":16:"61616161616161616161616161616161":"b91ce5ac77d33c234e61002ed6":"d5732582f494f5ddf35efd166c85af9c"

generic HMAC-MD2 Hash File OpenSSL test #2
depends_on:MBEDTLS_MD2_C
mbedtls_md_hmac:"MD2":16:"61616161616161616161616161616161":"270fcf11f27c27448457d7049a7edb084a3e554e0b2acf5806982213f0ad516402e4c869c4ff2171e18e3489baa3125d2c3056ebb616296f9b6aa97ef68eeabcdc0b6dde47775004096a241efcf0a90d19b34e898cc7340cdc940f8bdd46e23e352f34bca131d4d67a7c2ddb8d0d68b67f06152a128168e1c341c37e0a66c5018999b7059bcc300beed2c19dd1152d2fe062853293b8f3c8b5":"54ab68503f7d1b5c7741340dff2722a9"

generic
HMAC-MD2 Hash File OpenSSL test #3
depends_on:MBEDTLS_MD2_C
mbedtls_md_hmac:"MD2":16:"61616161616161616161616161616161616161616161616161616161616161616161616161616161616161616161616161616161616161616161616161616161616161616161616161616161616161616161616161616161616161616161":"b91ce5ac77d33c234e61002ed6":"d850e5f554558cf0fe79a0612e1d0365"

generic HMAC-MD4 Hash File OpenSSL test #1
depends_on:MBEDTLS_MD4_C
mbedtls_md_hmac:"MD4":16:"61616161616161616161616161616161":"b91ce5ac77d33c234e61002ed6":"eabd0fb
efb82fb0063a25a6d7b8bdc0f"

generic HMAC-MD4 Hash File OpenSSL test #2
depends_on:MBEDTLS_MD4_C
mbedtls_md_hmac:"MD4":16:"61616161616161616161616161616161":"270fcf11f27c27448457d7049a7edb084a3
e554e0b2acf5806982213f0ad516402e4c869c4ff2171e18e3489baa3125d2c3056ebb616296f9b6aa97ef68eeabcdc0b6
dde47775004096a241efcf0a90d19b34e898cc7340cdc940f8bdd46e23e352f34bca131d4d67a7c2ddb8d0d68b67f0615
2a128168e1c341c37e0a66c5018999b7059bcc300beed2c19dd1152d2fe062853293b8f3c8b5":"cec3c5e421a7b783aa
89cacf78daf6dc"

generic
HMAC-MD4 Hash File OpenSSL test #3
depends_on:MBEDTLS_MD4_C
mbedtls_md_hmac:"MD4":16:"61616161616161616161616161616161616161616161616161616161616161616161
61616161616161616161616161616161616161616161616161616161616161616161616161616161":"b91ce5ac77d33c234e61
002ed6":"ad5f0a04116109b397b57f9cc9b6df4b"

generic HMAC-MD5 Hash File OpenSSL test #1
depends_on:MBEDTLS_MD5_C
mbedtls_md_hmac:"MD5":16:"61616161616161616161616161616161":"b91ce5ac77d33c234e61002ed6":"425528
82f00bd4633ea81135a184b284"

generic HMAC-MD5 Hash File OpenSSL test #2
depends_on:MBEDTLS_MD5_C
mbedtls_md_hmac:"MD5":16:"61616161616161616161616161616161":"270fcf11f27c27448457d7049a7edb084a3
e554e0b2acf5806982213f0ad516402e4c869c4ff2171e18e3489baa3125d2c3056ebb616296f9b6aa97ef68eeabcdc0b6
dde47775004096a241efcf0a90d19b34e898cc7340cdc940f8bdd46e23e352f34bca131d4d67a7c2ddb8d0d68b67f0615
2a128168e1c341c37e0a66c5018999b7059bcc300beed2c19dd1152d2fe062853293b8f3c8b5":"a16a842891786d01fe
50ba7731db7464"

generic HMAC-MD5
Hash File OpenSSL test #3
depends_on:MBEDTLS_MD5_C
mbedtls_md_hmac:"MD5":16:"61616161616161616161616161616161616161616161616161616161616161616161
61616161616161616161616161616161616161616161616161616161616161616161616161616161":"b91ce5ac77d33c234e61
002ed6":"e97f623936f98a7f741c4bd0612fecc2"

HMAC-MD2 Bouncy Castle test #1
depends_on:MBEDTLS_MD2_C
mbedtls_md_hmac:"MD2":16:"0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b":"4869205468657265":"dc1923ef
5f161d35bef839ca8c807808"

HMAC-MD4 Bouncy Castle test #1
depends_on:MBEDTLS_MD4_C

mbedtls_md_hmac:"MD4":16:"0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b":"4869205468657265":"5570ce964ba8c11756cdc3970278ff5a"

HMAC-MD5 Bouncy Castle test #1
depends_on:MBEDTLS_MD5_C
mbedtls_md_hmac:"MD5":16:"0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b":"4869205468657265":"5ccec34ea9656392457fa1ac27f08fbc"

generic HMAC-MD5 Test Vector RFC2202 #1
depends_on:MBEDTLS_MD5_C
mbedtls_md_hmac:"MD5":16:"0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b":"4869205468657265":"9294727a3638bb1c13f48ef8158bfc9d"

generic
HMAC-MD5 Test Vector RFC2202 #2
depends_on:MBEDTLS_MD5_C
mbedtls_md_hmac:"MD5":16:"4a656665":"7768617420646f2079612077616e7420666f72206e6f7468696e673f":"750c783e6ab0b503eaa86e310a5db738"

generic HMAC-MD5 Test Vector RFC2202 #3
depends_on:MBEDTLS_MD5_C
mbedtls_md_hmac:"MD5":16:"aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa":"dddddd

6e67204c617267657220546861e20426c6f636b2d53697a65204b657920616e64204c617267657220546861e204f6e6520426c6f636b2d53697a652044617461":"6f630fad67cda0ee1fb1f562db3aa53e"

generic HMAC-RIPEMD160 Test vector RFC 2286 #1
depends_on:MBEDTLS_RIPEMD160_C
mbedtls_md_hmac:"RIPEMD160":20:"0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b":"4869205468657265":"24cb4bd67d20fc1a5d2ed7732dcc39377f0a5668"

generic
HMAC-RIPEMD160 Test vector RFC 2286 #2
depends_on:MBEDTLS_RIPEMD160_C
mbedtls_md_hmac:"RIPEMD160":20:"4a656665":"7768617420646f2079612077616e7420666f72206e6f7468696e673f":"dda6c0213a485a9e24f4742064a7f033b43c4069"

generic HMAC-RIPEMD160 Test vector RFC 2286 #3
depends_on:MBEDTLS_RIPEMD160_C
mbedtls_md_hmac:"RIPEMD160":20:"aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa":"ddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddd":"b0b105360de759960ab4f35298e116e295d8e7c1"

generic HMAC-RIPEMD160 Test vector RFC 2286 #4
depends_on:MBEDTLS_RIPEMD160_C
mbedtls_md_hmac:"RIPEMD160":20:"0102030405060708090a0b0c0d0e0f10111213141516171819":"cdcdcdc

RFC1319 #1
depends_on:MBEDTLS_MD_C:MBEDTLS_MD2_C
md_text_multi:"MD2":"":"8350e5a3e24c153df2275c9f80692773"

generic multi step mbedtls_md2 Test vector RFC1319 #2
depends_on:MBEDTLS_MD2_C
md_text_multi:"MD2":"a":"32ec01ec4a6dac72c0ab96fb34c0b5d1"

generic multi step mbedtls_md2 Test vector RFC1319 #3
depends_on:MBEDTLS_MD2_C
md_text_multi:"MD2":"abc":"da853b0d3f88d99b30283a69e6ded6bb"

generic multi step mbedtls_md2 Test vector RFC1319 #4
depends_on:MBEDTLS_MD2_C
md_text_multi:"MD2":"message digest":"ab4f496bfb2a530b219ff33031fe06b0"

generic multi step mbedtls_md2 Test vector RFC1319 #5
depends_on:MBEDTLS_MD2_C
md_text_multi:"MD2":"abcdefghijklmnopqrstuvwxyz":"4e8ddff3650292ab5a4108c3aa47940b"

generic multi step mbedtls_md2 Test vector RFC1319 #6
depends_on:MBEDTLS_MD2_C
md_text_multi:"MD2":"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789":"da3
3def2a42df13975352846c30338cd"

generic multi step mbedtls_md2 Test vector RFC1319 #7
depends_on:MBEDTLS_MD2_C
md_text_multi:"MD2":"12345678901234567890123456789012345678901234567890123456789012345678901234
567890":"d5976f79d83d3a0dc9806c3c66f3efd8"

generic
multi step mbedtls_md4 Test vector RFC1320 #1
depends_on:MBEDTLS_MD4_C
md_text_multi:"MD4":"":"31d6cfe0d16ae931b73c59d7e0c089c0"

generic multi step mbedtls_md4 Test vector RFC1320 #2
depends_on:MBEDTLS_MD4_C
md_text_multi:"MD4":"a":"bde52cb31de33e46245e05fbdbd6fb24"

generic multi step mbedtls_md4 Test vector RFC1320 #3
depends_on:MBEDTLS_MD4_C
md_text_multi:"MD4":"abc":"a448017aaf21d8525fc10ae87aa6729d"

generic multi step mbedtls_md4 Test vector RFC1320 #4
depends_on:MBEDTLS_MD4_C
md_text_multi:"MD4":"message digest":"d9130a8164549fe818874806e1c7014b"

generic multi step mbedtls_md4 Test vector RFC1320 #5

depends_on:MBEDTLS_MD4_C
md_text_multi:"MD4":"abcdefghijklmnopqrstuvwxyz":"d79e1c308aa5bbcdeea8ed63df412da9"

generic multi step mbedtls_md4 Test vector RFC1320 #6
depends_on:MBEDTLS_MD4_C
md_text_multi:"MD4":"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789":"043f8582f241db351ce627e153e7f0e4"

generic
multi step mbedtls_md4 Test vector RFC1320 #7
depends_on:MBEDTLS_MD4_C
md_text_multi:"MD4":"12345678901234567890123456789012345678901234567890123456789012345678901234567890":"e33b4ddc9c38f2199c3e7b164fcc0536"

generic multi step mbedtls_md5 Test vector RFC1321 #1
depends_on:MBEDTLS_MD5_C
md_text_multi:"MD5":"":"d41d8cd98f00b204e9800998ecf8427e"

generic multi step mbedtls_md5 Test vector RFC1321 #2
depends_on:MBEDTLS_MD5_C
md_text_multi:"MD5":"a":"0cc175b9c0f1b6a831c399e269772661"

generic multi step mbedtls_md5 Test vector RFC1321 #3
depends_on:MBEDTLS_MD5_C
md_text_multi:"MD5":"abc":"900150983cd24fb0d6963f7d28e17f72"

generic multi step mbedtls_md5 Test vector RFC1321 #4
depends_on:MBEDTLS_MD5_C
md_text_multi:"MD5":"message digest":"f96b697d7cb7938d525a2f31aaf161d0"

generic multi step mbedtls_md5 Test vector RFC1321 #5
depends_on:MBEDTLS_MD5_C
md_text_multi:"MD5":"abcdefghijklmnopqrstuvwxyz":"c3fcd3d76192e4007dfb496cca67e13b"

generic
multi step mbedtls_md5 Test vector RFC1321 #6
depends_on:MBEDTLS_MD5_C
md_text_multi:"MD5":"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789":"d174ab98d277d9f5a5611c2c9f419d9f"

generic multi step mbedtls_md5 Test vector RFC1321 #7
depends_on:MBEDTLS_MD5_C
md_text_multi:"MD5":"12345678901234567890123456789012345678901234567890123456789012345678901234567890":"57edf4a22be3c955ac49da2e2107b67a"

generic multi step mbedtls_ripemd160 Test vector from paper #1
depends_on:MBEDTLS_RIPEMD160_C
md_text_multi:"RIPEMD160":"":"9c1185a5c5e9fc54612808977ee8f548b2258d31"

generic multi step mbedtls_ripemd160 Test vector from paper #2
depends_on:MBEDTLS_RIPEMD160_C
md_text_multi:"RIPEMD160":"a":"0bdc9d2d256b3ee9daae347be6f4dc835a467ffe"

generic multi step mbedtls_ripemd160 Test vector from paper #3
depends_on:MBEDTLS_RIPEMD160_C
md_text_multi:"RIPEMD160":"abc":"8eb208f7e05d987a9b044a8e98c6b087f15a0bfc"

generic multi step mbedtls_ripemd160 Test vector from paper #4
depends_on:MBEDTLS_RIPEMD160_C
md_text_multi:"RIPEMD160":"message
digest":"5d0689ef49d2fae572b881b123a85ffa21595f36"

generic multi step mbedtls_ripemd160 Test vector from paper #5
depends_on:MBEDTLS_RIPEMD160_C
md_text_multi:"RIPEMD160":"abcdefghijklmnopqrstuvwxyz":"f71c27109c692c1b56bbdceb5b9d2865b3708dbc"

generic multi step mbedtls_ripemd160 Test vector from paper #6
depends_on:MBEDTLS_RIPEMD160_C
md_text_multi:"RIPEMD160":"abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq":"12a053384a9c0c88e405a06c27dcf49ada62eb2b"

generic multi step mbedtls_ripemd160 Test vector from paper #7
depends_on:MBEDTLS_RIPEMD160_C
md_text_multi:"RIPEMD160":"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789":"b0e20b6e3116640286ed3a87a5713079b21f5189"

generic multi step mbedtls_ripemd160 Test vector from paper #8
depends_on:MBEDTLS_RIPEMD160_C
md_text_multi:"RIPEMD160":"12345678901234567890123456789012345678901234567890123456789012345678901234567890":"9b752e45573d4b39f4dbd3323cab82bf63326bfb"

generic
multi step HMAC-MD2 Hash File OpenSSL test #1
depends_on:MBEDTLS_MD2_C
md_hmac_multi:"MD2":16:"61616161616161616161616161616161":"b91ce5ac77d33c234e61002ed6":"d5732582f494f5ddf35efd166c85af9c"

generic multi step HMAC-MD2 Hash File OpenSSL test #2
depends_on:MBEDTLS_MD2_C
md_hmac_multi:"MD2":16:"61616161616161616161616161616161":"270fcf11f27c27448457d7049a7edb084a3e554e0b2acf5806982213f0ad516402e4c869c4ff2171e18e3489baa3125d2c3056ebb616296f9b6aa97ef68eeabcdc0b6dde47775004096a241efcf0a90d19b34e898cc7340cdc940f8bdd46e23e352f34bca131d4d67a7c2ddb8d0d68b67f06152a128168e1c341c37e0a66c5018999b7059bcc300beed2c19dd1152d2fe062853293b8f3c8b5":"54ab68503f7d1b5c7741340dff2722a9"

generic multi step HMAC-MD2 Hash File OpenSSL test #3

depends_on:MBEDTLS_MD2_C
md_hmac_multi:"MD2":16:"61616161616161616161

md_hmac_multi:"MD5":16:"0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b":"4869205468657265":"9294727a3638bb1c13f48ef8158bfc9d"

generic multi step HMAC-MD5 Test Vector RFC2202 #2
depends_on:MBEDTLS_MD5_C
md_hmac_multi:"MD5":16:"4a656665":"7768617420646f2079612077616e7420666f72206e6f7468696e673f":"750c783e6ab0b503eaa86e310a5db738"

generic multi step HMAC-MD5 Test Vector RFC2202 #3
depends_on:MBEDTLS_MD5_C
md_hmac_multi:"MD5":16:"aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa":"ddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddd":"56be34521d144c88dbb8c733f0e8b3f6"

generic multi step HMAC-MD5 Test Vector RFC2202 #4
depends_on:MBEDTLS_MD5_C
md_hmac_multi:"MD5":16:"0102030405060708090a0b0c0d0e0f10111213141516171819":"cdcdcdc

md_hmac_multi:"RIPEMD160":20:"4a656665":"7768617420646f2079612077616e7420666f72206e6f7468696e673f":"dda6c0213a485a9e24f4742064a7f033b43c4069"

generic multi step HMAC-RIPEMD160 Test vector RFC 2286 #3
depends_on:MBEDTLS_RIPEMD160_C
md_hmac_multi:"RIPEMD160":20:"aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa":"dddddd

generic MD2 Hash file #4
depends_on:MBEDTLS_MD2_C
mbedtls_md_file:"MD2":"data_files/hash_file_4":"8350e5a3e24c153df2275c9f80692773"

generic MD4 Hash file #1
depends_on:MBEDTLS_MD4_C
mbedtls_md_file:"MD4":"data_files/hash_file_1":"8d19772c176bd27153b9486715e2c0b9"

generic MD4 Hash file #2
depends_on:MBEDTLS_MD4_C
mbedtls_md_file:"MD4":"data_files/hash_file_2":"f2ac53b8542882a5a0007c6f84b4d9fd"

generic
MD4 Hash file #3
depends_on:MBEDTLS_MD4_C
mbedtls_md_file:"MD4":"data_files/hash_file_3":"195c15158e2d07881d9a654095ce4a42"

generic MD4 Hash file #4
depends_on:MBEDTLS_MD4_C
mbedtls_md_file:"MD4":"data_files/hash_file_4":"31d6cfe0d16ae931b73c59d7e0c089c0"

generic MD5 Hash file #1
depends_on:MBEDTLS_MD5_C
mbedtls_md_file:"MD5":"data_files/hash_file_1":"52bcdc983c9ed64fc148a759b3c7a415"

generic MD5 Hash file #2
depends_on:MBEDTLS_MD5_C
mbedtls_md_file:"MD5":"data_files/hash_file_2":"d17d466f15891df10542207ae78277f0"

generic MD5 Hash file #3
depends_on:MBEDTLS_MD5_C
mbedtls_md_file:"MD5":"data_files/hash_file_3":"d945bcc6200ea95d061a2a818167d920"

generic MD5 Hash file #4
depends_on:MBEDTLS_MD5_C
mbedtls_md_file:"MD5":"data_files/hash_file_4":"d41d8cd98f00b204e9800998ecf8427e"

generic RIPEMD160 Hash file #0 (from paper)
depends_on:MBEDTLS_RIPEMD160_C
mbedtls_md_file:"RIPEMD160":"data_files/hash_file_5":"52783243c1697bdbe16d37f97f68f08325dc1528"

generic
RIPEMD160 Hash file #1
depends_on:MBEDTLS_RIPEMD160_C
mbedtls_md_file:"RIPEMD160":"data_files/hash_file_1":"82f1d072f0ec0c2b353703a7b575a04c113af1a6"

generic RIPEMD160 Hash file #2
depends_on:MBEDTLS_RIPEMD160_C

mbedtls_md_file:"RIPEMD160":"data_files/hash_file_2":"996fbc8b79206ba7393ebcd246584069b1c08f0f"

generic RIPEMD160 Hash file #3
depends_on:MBEDTLS_RIPEMD160_C
mbedtls_md_file:"RIPEMD160":"data_files/hash_file_3":"8653b46d65998fa8c8846efa17937e742533ae48"

generic RIPEMD160 Hash file #4
depends_on:MBEDTLS_RIPEMD160_C
mbedtls_md_file:"RIPEMD160":"data_files/hash_file_4":"9c1185a5c5e9fc54612808977ee8f548b2258d31"

generic HMAC-SHA-1 Test Vector FIPS-198a #1
depends_on:MBEDTLS_SHA1_C
mbedtls_md_hmac:"SHA1":20:"000102030405060708090a0b0c0d0e0f10111213141516171819 1a1b1c1d1e1f2021 22232425262728292a2b2c2d2e2f303132333435363738393a3b3c3d3e3f":"53616d706c65202331":"4f4ca3d5d68ba 7cc0a1208c9c61e9c5da0403c0a"

generic HMAC-SHA-1 Test Vector FIPS-198a #2
depends_on:MBEDTLS_SHA1_C
mbedtls_md_hmac:"SHA1":20:"303132333435363738393a3b3c3d3e3f40414243":"53616d706c65202332":"0922d 3405faa3d194f82a45830737d5cc6c75d24"

generic
HMAC-SHA-1 Test Vector FIPS-198a #3
depends_on:MBEDTLS_SHA1_C
mbedtls_md_hmac:"SHA1":20:"505152535455565758595a5b5c5d5e5f606162636465666768696a6b6c6d6e6f7071 72737475767778797a7b7c7d7e7f808182838485868788898a8b8c8d8e8f909192939495969798999a9b9c9d9e9fa0a 1a2a3a4a5a6a7a8a9aaabacadaeafb0b1b2b3":"53616d706c65202333":"bcf41eab8bb2d802f3d05caf7cb092ecf8d1a3a a"

generic HMAC-SHA-1 Test Vector FIPS-198a #4
depends_on:MBEDTLS_SHA1_C
mbedtls_md_hmac:"SHA1":12:"707172737475767778797a7b7c7d7e7f808182838485868788898a8b8c8d8e8f9091 92939495969798999a9b9c9d9e9fa0":"53616d706c65202334":"9ea886efe268dbecce420c75"

generic HMAC-SHA-1 Test Vector NIST CAVS #1
depends_on:MBEDTLS_SHA1_C
mbedtls_md_hmac:"SHA1":10:"7b10f4124b15c82e":"27dcb5b1daf60cfd3e2f73d4d64ca9c684f8bf71fc682a46793b 1790afa4feb100ca7aaff26f58f0e1d0ed42f1cdad1f474afa2e79d53a0c42892c4d7b327cbe46b295ed8da3b6ecab3d485 1687a6f812b79df2f6b20f11f6706f5301790ca99625aad7391d84f78043d2a0a239b1477984c157bbc9276064e7a1a40 6b0612ca":"4ead12c2fe3d6ea43acb"

generic
HMAC-SHA-1 Test Vector NIST CAVS #2
depends_on:MBEDTLS_SHA1_C
mbedtls_md_hmac:"SHA1":10:"4fe9fb902172a21b":"4ceb3a7c13659c22fe51134f03dce4c239d181b63c6b0b59d36 7157fd05cab98384f92dfa482d2d5e78e72eef1b1838af4696026c54233d484ecbbe87f904df5546419f8567eafd232e6c 2fcd3ee2b7682c63000524b078dbb2096f585007deae752562df1fe3b01278089e16f3be46e2d0f7cabac2d8e6cc02a2d 0ca953425f":"564428a67be1924b5793"

generic HMAC-SHA-1 Test Vector NIST CAVS #3
depends_on:MBEDTLS_SHA1_C
mbedtls_md_hmac:"SHA1":10:"d1f01455f78c4fb4":"00d40f67b57914bec456a3e3201ef1464be319a8d188c02e157af4b54f9b5a66d67f898a9bdbb19ff63a80aba6f246d013575721d52eb1b47a65def884011c49b257bcc2817fc853f106e8138ce386d7a5ac3103de0a3fa0ed6bb7af9ff66ebd1cc46fb86e4da0013d20a3c2dcd8fb828a4b70f7f104b41bf3f44682a66497ea":"56a665a7cdfe610f9fc5"

generic HMAC-SHA-1 Test Vector NIST CAVS #4
depends_on:MBEDTLS_SHA1_C
mbedtls_md_hmac:"SHA1":10:"4e5ef77fdf033a5b":"e59326464e3201d195e29f2a3446ec1b1c9ff31154e2a4d0e40ed466f1bc855d29f76835624fa0127d29c9b1915939a046f385af7e5d47a23ba91f28bd22f811ea258dbbf3332bcd3543b8285d5df41bd064ffd64a341c22c4edb44f9c8d9e6df0c59dbf4a052a6c83da7478e179a6f3839c6870ff8ca8b9497f9ac1d725fdda":"981c0a7a8423b63a8fa6"

generic
HMAC-SHA-1 Test Vector NIST CAVS #5
depends_on:MBEDTLS_SHA1_C
mbedtls_md_hmac:"SHA1":10:"bcd9ff8aa60be2be":"51be4d0eb37bab714f92e19e9d70390655b363e8cd346a748245e731f437759cb8206412c8dab2ef1d4f36f880f41ff69d949da4594fdecb65e23cac1329b59e69e29bf875b38c31df6fa546c595f35cc2192aa750679a8a51a65e00e839d73a8d8c598a610d237fbe78955213589d80efcb73b95b8586f96d17b6f51a71c3b8":"84633f9f5040c8971478"

generic HMAC-SHA-1 Test Vector NIST CAVS #6
depends_on:MBEDTLS_SHA1_C
mbedtls_md_hmac:"SHA1":10:"4a661bce6ed86d21":"5ff6c744f1aab1bc29697d71f67541b8b3cec3c7079183b10a83fb98a9ee251d4bac3e1cb581ca972aaed8efd7c2875a6fb4c991132f67c9742d45e53bc7e8eaa94b35b37a907be61086b426cd11088ac118934e85d968c9667fd69fc6f6ea38c0fe34710b7ece91211b9b7ea00acd31f022aa6726368f9928a1352f122233f1":"739df59353ac6694e55e"

generic
HMAC-SHA-1 Test Vector NIST CAVS #7
depends_on:MBEDTLS_SHA1_C
mbedtls_md_hmac:"SHA1":10:"1287e1565a57b547":"390ffdccc6171c11568d85b8f913e019bf4cd982ca9cd21ea730d41bdf3fcc0bc88ff48ba13a8f23deb2d96ec1033e7b2a58ca72b0c1e17bf03330db25d1e360fa6918009c4294bd1215b5ccd159a8f58bc3dc3d490eb7c3b9f887e8c98dbbb274a75373dcb695a59abd0219529d88518a96f92abc0bbcbda985c388f1fbbcc9":"d78ddf08077c7d9e2ba6"

generic HMAC-SHA-224 Test Vector NIST CAVS #1
depends_on:MBEDTLS_SHA256_C
mbedtls_md_hmac:"SHA224":14:"e055eb756697ee573fd3214811a9f7fa":"3875847012ee42fe54a0027bdf38cca7021b83a2ed0503af69ef6c37c637bc1114fba40096c5947d736e19b7af3c68d95a4e3b8b073adbbb80f47e9db8f2d4f0018ddd847fabfdf9dd9b52c93e40458977725f6b7ba15f0816bb895cdf50401268f5d702b7e6a5f9faef57b8768c8a3fc14f9a4b3182b41d940e337d219b29ff":"40a453133361cc48da11baf616ee"

generic HMAC-SHA-224 Test Vector
NIST CAVS #2
depends_on:MBEDTLS_SHA256_C

mbedtls_md_hmac:"SHA224":14:"88e5258b55b1623385eb9632fa7c57d6":"ada76bb604be14326551701cf30e48a6
5eee80b44f0b9d4a07b1844543b7844a621097fdc99de57387458ae9354899b620d0617eabcaefa9eef3d413a3362805
4335ce656c26fa2986e0f111a6351096b283101ec7868871d770b370973c7405983f9756b3005a3eab492cfd0e7eb42e
5c2e15fa6be8718c0a50acc4e5717230":"81c783af538015cef3c60095df53"

generic HMAC-SHA-224 Test Vector NIST CAVS #3
depends_on:MBEDTLS_SHA256_C
mbedtls_md_hmac:"SHA224":14:"85d402d822114d31abf75526e2538705":"8020d8d98cc2e2298b32879c51c751e1
dd5558fe2eabb8f158604297d6d072ce2261a1d6830b7cfe2617b57c7126f99c9476211d6161acd75d266da217ec8174
b80484c9dc6f0448a0a036a3fc82e8bf54bdb71549368258d5d41f57978a4c266b92e8783ef66350215573d99be40891
44b383ad8f3222bae8f3bf80ffb1bb2b":"2aa0340ac9deafe3be38129daca0"

generic HMAC-SHA-224 Test Vector NIST CAVS #4
depends_on:MBEDTLS_SHA256_C
mbedtls_md_hmac:"SHA224":14:"545c6eecc5ee46fa17c59f91a94f81ae":"8fb7f3565593170152ddb2021874784e95
1977cfdd22f8b72a72a61320a8f2a35697b5e913f717805559b1af1861ee3ed42fb788481e4fd276b17bdbefcae7b4501
dc5d20de5b7626dd5efdcd65294db4bdf682c33d9a9255c6435383fa5f1c886326a3acbc6bd50a33ab5b2dbb034ce011
2d4e226bbcd57e3731a519aa1d784":"3eb566eac54c4a3a9ef092469f24"

generic
HMAC-SHA-224 Test Vector NIST CAVS #5
depends_on:MBEDTLS_SHA256_C
mbedtls_md_hmac:"SHA224":14:"4466ab4dc438841a9750c7f173dff02e":"2534c11c78c99cffaec8f722f04adc7045c
7324d58ce98e37cfa94b6ed21ed7f58ce55379ef24b72d6d640ee9154f96c614734be9c408e225d7ba4cecc1179cc9f6e
1808e1067aa8f244a99bd0c3267594c1887a40d167f8b7cf78db0d19f97b01fc50b8c86def490dfa7a5135002c33e71d7
7a8cce8ea0f93e0580439a33733":"59f44a9bbed4875b892d22d6b5ab"

generic HMAC-SHA-224 Test Vector NIST CAVS #6
depends_on:MBEDTLS_SHA256_C
mbedtls_md_hmac:"SHA224":28:"0e3dd9bb5e4cf0f09a4c11600af56d8d":"f4589fa76c328ea25cf8bae582026ba40a
59d45a546ff31cf80eb826088f69bb954c452c74586836416dee90a5255bc5d56d3b405b3705a5197045688b32fa984c
3a3dfbdc9c2460a0b5e6312a624048bb6f170306535e9b371a3ab134a2642a230ad03d2c688cca80baeaee9a20e1d4c5
48b1cede29c6a45bf4df2c8c476f1a":"12175b93e3da4c58217145e4dc0a1cf142fab9319bb501e037b350ba"

generic
HMAC-SHA-224 Test Vector NIST CAVS #7
depends_on:MBEDTLS_SHA256_C
mbedtls_md_hmac:"SHA224":28:"cda5187b0c5dcb0f8e5a8beed2306584":"9011ae29b44c49b347487ce972965f16a
de3c15be0856ce9c853a9739dba07e4f20d594ddc1dfe21560a65a4e458cfa17745575b915a30c7a9412ff8d1d689db96
80dd2428c27588bb0dc92d2cd9445fe8f44b840a197c52c3c4333fff45533945134398df6436513cfab06c924046b8c79
5a5bd92e8d5f2de85bf306f2eed67":"4aaba92b40e2a600feab176eb9b292d814864195c03342aad6f67f08"

generic HMAC-SHA-256 Test Vector NIST CAVS #1
depends_on:MBEDTLS_SHA256_C
mbedtls_md_hmac:"SHA256":16:"cdffd34e6b16fdc0":"d83e78b99ab61709608972b36e76a575603db742269cc5dd4
e7d5ca7816e26b65151c92632550cb4c5253c885d5fce53bc47459a1dbd5652786c4aac0145a532f12c05138af04cbb5
58101a7af5df478834c2146594dd73690d01a4fe72545894335f427ac70204798068cb86c5a600b40b414ede23590b41
e1192373df84fe3":"c6f0dde266cb4a26d41e8259d33499cc"

generic
HMAC-SHA-256 Test Vector NIST CAVS #2
depends_on:MBEDTLS_SHA256_C
mbedtls_md_hmac:"SHA256":16:"6d97bb5892245be2":"13c2b391d59c0252ca5d2302beaaf88c4bcd779bb505ad9a122003dfae4cc123ad2bd036f225c4f040021a6b9fb8bd6f0281cf2e2631a732bdc71693cc42ef6d52b6c6912a9ef77b3274eb85ad7f965ae6ed44ac1721962a884ec7acfb4534b1488b1c0c45afa4dae8da1eb7b0a88a3240365d7e4e7d826abbde9f9203fd99d7":"31588e241b015319a5ab8c4527296498"

generic HMAC-SHA-256 Test Vector NIST CAVS #3
depends_on:MBEDTLS_SHA256_C
mbedtls_md_hmac:"SHA256":16:"3c7fc8a70b49007a":"60024e428a39c8b8bb2e9591bad9dc2115dfbfd716b6eb7af30a6eb34560caccbbfa47b710fa8d523aca71e9e5ba10fc1feb1a43556d71f07ea4f33496f093044e8caf1d02b79e46eb1288d5964a7a7494f6b92574c35784eece054c6151281d80822f7d47b8231c35d07f5cb5cf4310ddc844845a01c6bfab514c048eccaf9f":"1c98c94a32bec9f253c21070f82f8438"

generic HMAC-SHA-256 Test Vector NIST CAVS #4
depends_on:MBEDTLS_SHA256_C
mbedtls_md_hmac:"SHA256":24:"369f33f85b927a07":"ae8e2a94ca386d448cbacdb0e9040ae3cb297c296363052cc157455da29a0c95897315fc11e3f12b81e2418da1ec280bccbc00e847584ce9d14deeba7b3c9b8dba958b04bba37551f6c9ba9c060be1a4b8cf43aa62e5078b76c6512c5619b71a6a7cf5727180e1ff14f5a1a3c1691bf8b6ebad365c151e58d749d57adb3a4986":"60b90383286533d309de46593e6ce39fc51fb00a8d88278c"

generic
HMAC-SHA-256 Test Vector NIST CAVS #5
depends_on:MBEDTLS_SHA256_C
mbedtls_md_hmac:"SHA256":24:"e5179687582b4dc4":"ce103bdacdf32f614f6727bcb31ca1c2824a850d00f5585b016fb234fe1ef2cd687f302d3c6b738ed89a24060d65c36675d0d96307c72ef3e8a83bfa8402e226de9d5d1724ba75c4879bf41a4a465ce61887d9f49a34757849b48bae81c27ebed76faae2ad669bca04747d409148d40812776e0ae2c395b3cb9c89981ce72d5c":"509581f6816df4b8cc9f2cf42b7cc6e6a5a1e375a16f2412"

generic HMAC-SHA-256 Test Vector NIST CAVS #6
depends_on:MBEDTLS_SHA256_C
mbedtls_md_hmac:"SHA256":24:"63cec6246aeb1b61":"c178db908a405fa88aa255b8cad22b4057016585f139ee930388b083d86062fa0b3ea1f23f8a43bd11bee8464bcbd19b5ab9f6a8038d5245516f8274d20c8ee3033a07b908da528fa00343bb595deed500cab9745c4cb6391c23300f0d3584b090b3326c4cfa342620b78f9f5b4f27f7307ed770643ec1764aeae3dcf1a3ec69":"64f3dd861b7c7d29fce9ae0ce9ed954b5d7141806ee9eec7"

generic
HMAC-SHA-384 Test Vector NIST CAVS #1
depends_on:MBEDTLS_SHA512_C
mbedtls_md_hmac:"SHA384":32:"91a7401817386948ca952f9a20ee55dc":"2fea5b91035d6d501f3a834fa178bff4e64b99a8450432dafd32e4466b0e1e7781166f8a73f7e036b3b0870920f559f47bd1400a1a906e85e0dcf00a6c26862e9148b23806680f285f1fe4f93cdaf924c181a965465739c14f2268c8be8b471847c74b222577a1310bcdc1a85ef1468aa1a3fd4031213c97324b7509c9050a3d":"6d7be9490058cf413cc09fd043c224c2ec4fa7859b13783000a9a593c9f75838"

generic HMAC-SHA-384 Test Vector NIST CAVS #2
depends_on:MBEDTLS_SHA512_C

mbedtls_md_hmac:"SHA384":32:"d6cac19657061aa90a6da11cd2e9ea47":"9f482e4655173135dfaa22a11bbbe6af2
63db48716406c5aec162ba3c4b41cad4f5a91558377521191c7343118beee65982929802913d67b6de5c4bdc3d27299
bd722219d5ad2efa5bdb9ff7b229fc4bbc3f60719320cf2e7a51cad1133d21bad2d80919b1836ef825308b7c51c6b7677
ac782e2bc30007afba065681cbdd215":"f3d5f3c008175321aa7b2ea379eaa4f8b9dcc60f895ec8940b8162f80a7dfe9f"

generic
HMAC-SHA-384 Test Vector NIST CAVS #3
depends_on:MBEDTLS_SHA512_C
mbedtls_md_hmac:"SHA384":32:"e06366ad149b8442cd4c1abdddd0afde":"2d140a194c02a5598f69174834679b83
71234a0d505491f1bd03e128dd91a8bca2fb812e9d5da71613b5b00952ea78bf450d5b7547dea79135925085c7d3e6f5
2009c51ca3d88c6c09e9d074b0ee110736e0ec9b478b93efb34d7bf1c41b54dececc43eab077a3aa4998ede53f67b4ea36
c266745f9643d5360bdc8337c70dabf":"c19c67eda6fe29f3667bee1c897c333ce7683094ae77e84b4c16378d290895a
1"

generic HMAC-SHA-384 Test Vector NIST CAVS #4
depends_on:MBEDTLS_SHA512_C
mbedtls_md_hmac:"SHA384":48:"01ac59f42f8bb91d1bd10fe6990d7a87":"3caf18c476edd5615f343ac7b7d3a9da9e
fade755672d5ba4b8ae8a7505539ea2c124ff755ec0457fbe49e43480b3c71e7f4742ec3693aad115d039f90222b030fdc
9440313691716d5302005808c07627483b916fdf61983063c2eb1268f2deeef42fc790334456bc6bad256e31fc9066de
7cc7e43d1321b1866db45e905622":"1985fa2163a5943fc5d92f1fe8831215e7e91f0bff5332bc713a072bdb3a8f9e5c5
157463a3bfeb36231416e65973e64"

generic
HMAC-SHA-384 Test Vector NIST CAVS #5
depends_on:MBEDTLS_SHA512_C
mbedtls_md_hmac:"SHA384":48:"fd74b9d9e102a3a80df1baf0cb35bace":"1a068917584813d1689ccbd0370c2114d
537cdc8cc52bf6db16d5535f8f7d1ad0c850a9fa0cf62373ffbf7642b1f1e8164010d350721d798d9f99e9724830399c2f
ce26377e83d38845675457865c03d4a07d741a505ef028343eb29fd46d0f761f3792886998c1e5c32ac3bc7e6f08faed1
94b34f06eff4d5d4a5b42c481e0e":"a981eaf5de3d78b20ebd4414a4edd0657e3667cd808a0dbc430cf7252f73a5b24ef
a136039207bd59806897457d74e0c"

generic HMAC-SHA-384 Test Vector NIST CAVS #5
depends_on:MBEDTLS_SHA512_C
mbedtls_md_hmac:"SHA384":48:"9fe794f0e26b669fa5f6883149377c6c":"6010c9745e8f1d44cfdc99e7e0fd79bc42
71944c2d1d84dba589073dfc4ca5eb98c59356f60cd87bef28aeb83a832bde339b2087daf942aa1f67876c5d5ed33924b
ed4143bc12a2be532ccaf64daa7e2bc3c8872b9823b0533b6f5159135effe8c61545536975d7c3a61ba7365ec35f165bc
92b4d19eb9156ade17dfa1bb4161":"915ae61f8754698c2b6ef9629e93441f8541bd4258a5e05372d19136cfaefc0473b
48d96119291b38eb1a3cb1982a986"

generic
HMAC-SHA-512 Test Vector NIST CAVS #1
depends_on:MBEDTLS_SHA512_C
mbedtls_md_hmac:"SHA512":32:"c95a17c09940a691ed2d621571b0eb844ede55a9":"99cd28262e81f34878cdcebf4
128e05e2098a7009278a66f4c785784d0e5678f3f2b22f86e982d273b6273a222ec61750b4556d766f1550a7aedfe83fa
edbc4bdae83fa560d62df17eb914d05fdaa48940551bac81d700f5fca7147295e386e8120d66742ec65c6ee8d89a92217
a0f6266d0ddc60bb20ef679ae8299c8502c2f":"6bc1379d156559ddee2ed420ea5d5c5ff3e454a1059b7ba72c350e77b6
e9333c"

generic HMAC-SHA-512 Test Vector NIST CAVS #2
depends_on:MBEDTLS_SHA512_C
mbedtls_md_hmac:"SHA512":32:"3b10b8fa718840d1dea8e9fc317476bcf55875fd":"f04f5b7073d7d0274e8354433b390306c5607632f5f589c12edb62d55673aff2366d2e6b24de731adf92e654baa30b1cfd4a069788f65ec1b99b015d904d8832110dbd74eae35a81562d14ce4136d820ad0a55ff5489ba678fbbc1c27663ec1349d70e740f0e0ec27cfbe8971819f4789e486b50a2d7271d77e2aaea50de62fd":"fc3c38c7a17e3ce06db033f1c172866f01a00045db55f2e234f71c82264f2ba2"

generic HMAC-SHA-512 Test Vector NIST
CAVS #3
depends_on:MBEDTLS_SHA512_C
mbedtls_md_hmac:"SHA512":32:"4803d311394600dc1e0d8fc8cedeb8bde3fe7c42":"a10c125dd702a97153ad923ba5e9889cfac1ba169de370debe51f233735aa6effcc9785c4b5c7e48c477dc5c411ae6a959118584e26adc94b42c2b29b046f3cf01c65b24a24bd2e620bdf650a23bb4a72655b1100d7ce9a4dab697c6379754b4396c825de4b9eb73f2e6a6c0d0353bbdeaf706612800e137b858fdb30f3311c6":"7cd8236c55102e6385f52279506df6fcc388ab75092da21395ce14a82b202ffa"

generic HMAC-SHA-512 Test Vector NIST CAVS #4
depends_on:MBEDTLS_SHA512_C
mbedtls_md_hmac:"SHA512":48:"aeb2f3b977fa6c8e71e07c5a5c74ff58166de092":"22457355dc76095abd46846b41cfe49a06ce42ac8857b4702fc771508dfb3626e0bfe851df897a07b36811ec433766e4b4166c26301b3493e7440d4554b0ef6ac20f1a530e58fac8aeba4e9ff2d4898d8a28783b49cd269c2965fd7f8e4f2d60cf1e5284f2495145b72382aad90e153a90ecae125ad75336fb128825c23fb8b0":"fa39bd8fcc3bfa218f9dea5d3b2ce10a7619e31678a56d8a9d927b1fe703b125af445debe9a89a07db6194d27b44d85a"

generic HMAC-SHA-512 Test Vector NIST CAVS #5
depends_on:MBEDTLS_SHA512_C
mbedtls_md_hmac:"SHA512":48:"4285d3d7744da52775bb44ca436a3154f7980309":"208f0b6f2de2e5aa5df11927ddc6df485edc1193181c484d0f0a434a95418803101d4de9fdb798f93516a6916fa38a8207de1666fe50fe3441c03b112eaaae6954ed063f7ac4e3c1e3f73b20d153fe9e4857f5e91430f0a70ee820529adac2467469fd18adf10e2af0fea27c0abc83c5a9af77c364a466cffce8bab4e2b70bc1":"fe7603f205b2774fe0f14ecfa3e338e90608a806d11ca459dff5ce36b1b264ecd3af5f0492a7521d8da3102ba20927a5"

generic
HMAC-SHA-512 Test Vector NIST CAVS #6
depends_on:MBEDTLS_SHA512_C
mbedtls_md_hmac:"SHA512":48:"8ab783d5acf32efa0d9c0a21abce955e96630d89":"17371e013dce839963d54418e97be4bd9fa3cb2a368a5220f5aa1b8aaddfa3bdefc91afe7c717244fd2fb640f5cb9d9bf3e25f7f0c8bc758883b89dcdce6d749d9672fed222277ece3e84b3ec01b96f70c125fcb3cbee6d19b8ef0873f915f173bdb05d81629ba187cc8ac1934b2f75952fb7616ae6bd812946df694bd2763af":"9ac7ca8d1aefc166b046e4cf7602ebe181a0e5055474bff5b342106731da0d7e48e4d87bc0a6f05871574289a1b099f8"

generic multi step HMAC-SHA-1 Test Vector FIPS-198a #1
depends_on:MBEDTLS_SHA1_C
md_hmac_multi:"SHA1":20:"000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f20212223242526272829 2a2b2c2d2e2f303132333435363738393a3b3c3d3e3f":"53616d706c65202331":"4f4ca3d5d68ba7cc0a1208c9c61e9c5da0403c0a"

generic
multi step HMAC-SHA-1 Test Vector FIPS-198a #2
depends_on:MBEDTLS_SHA1_C
md_hmac_multi:"SHA1":20:"303132333435363738393a3b3c3d3e3f40414243":"53616d706c65202332":"0922d34
05faa3d194f82a45830737d5cc6c75d24"

generic multi step HMAC-SHA-1 Test Vector FIPS-198a #3
depends_on:MBEDTLS_SHA1_C
md_hmac_multi:"SHA1":20:"505152535455565758595a5b5c5d5e5f606162636465666768696a6b6c6d6e6f707172
737475767778797a7b7c7d7e7f808182838485868788898a8b8c8d8e8f909192939495969798999a9b9c9d9e9fa0a1a
2a3a4a5a6a7a8a9aaabacadaeafb0b1b2b3":"53616d706c65202333":"bcf41eab8bb2d802f3d05caf7cb092ecf8d1a3aa"

generic multi step HMAC-SHA-1 Test Vector FIPS-198a #4
depends_on:MBEDTLS_SHA1_C
md_hmac_multi:"SHA1":12:"707172737475767778797a7b7c7d7e7f808182838485868788898a8b8c8d8e8f909192
939495969798999a9b9c9d9e9fa0":"53616d706c65202334":"9ea886efe268dbecce420c75"

generic
multi step HMAC-SHA-1 Test Vector NIST CAVS #1
depends_on:MBEDTLS_SHA1_C
md_hmac_multi:"SHA1":10:"7b10f4124b15c82e":"27dcb5b1daf60cfd3e2f73d4d64ca9c684f8bf71fc682a46793b17
90afa4feb100ca7aaff26f58f0e1d0ed42f1cdad1f474afa2e79d53a0c42892c4d7b327cbe46b295ed8da3b6ecab3d48516
87a6f812b79df2f6b20f11f6706f5301790ca99625aad7391d84f78043d2a0a239b1477984c157bbc9276064e7a1a406b
0612ca":"4ead12c2fe3d6ea43acb"

generic multi step HMAC-SHA-1 Test Vector NIST CAVS #2
depends_on:MBEDTLS_SHA1_C
md_hmac_multi:"SHA1":10:"4fe9fb902172a21b":"4ceb3a7c13659c22fe51134f03dce4c239d181b63c6b0b59d3671
57fd05cab98384f92dfa482d2d5e78e72eef1b1838af4696026c54233d484ecbbe87f904df5546419f8567eafd232e6c2f
cd3ee2b7682c63000524b078dbb2096f585007deae752562df1fe3b01278089e16f3be46e2d0f7cabac2d8e6cc02a2d0c
a953425f":"564428a67be1924b5793"

generic multi step HMAC-SHA-1 Test Vector NIST CAVS #3
depends_on:MBEDTLS_SHA1_C
md_hmac_multi:"SHA1":10:"d1f01455f78c4fb4":"00d40f67b57914bec456a3e3201ef1464be319a8d188c02e157af4
b54f9b5a66d67f898a9bdbb19ff63a80aba6f246d013575721d52eb1b47a65def884011c49b257bcc2817fc853f106e81
38ce386d7a5ac3103de0a3fa0ed6bb7af9ff66ebd1cc46fb86e4da0013d20a3c2dcd8fb828a4b70f7f104b41bf3f44682a6
6497ea":"56a665a7cdfe610f9fc5"

generic
multi step HMAC-SHA-1 Test Vector NIST CAVS #4
depends_on:MBEDTLS_SHA1_C
md_hmac_multi:"SHA1":10:"4e5ef77fdf033a5b":"e59326464e3201d195e29f2a3446ec1b1c9ff31154e2a4d0e40ed4
66f1bc855d29f76835624fa0127d29c9b1915939a046f385af7e5d47a23ba91f28bd22f811ea258dbbf3332bcd3543b82
85d5df41bd064ffd64a341c22c4edb44f9c8d9e6df0c59dbf4a052a6c83da7478e179a6f3839c6870ff8ca8b9497f9ac1d
725fdda":"981c0a7a8423b63a8fa6"

generic multi step HMAC-SHA-1 Test Vector NIST CAVS #5

depends_on:MBEDTLS_SHA1_C
md_hmac_multi:"SHA1":10:"bcd9ff8aa60be2be":"51be4d0eb37bab714f92e19e9d70390655b363e8cd346a748245e731f437759cb8206412c8dab2ef1d4f36f880f41ff69d949da4594fdecb65e23cac1329b59e69e29bf875b38c31df6fa546c595f35cc2192aa750679a8a51a65e00e839d73a8d8c598a610d237fbe78955213589d80efcb73b95b8586f96d17b6f51a71c3b8":"84633f9f5040c8971478"

generic
multi step HMAC-SHA-1 Test Vector NIST CAVS #6
depends_on:MBEDTLS_SHA1_C
md_hmac_multi:"SHA1":10:"4a661bce6ed86d21":"5ff6c744f1aab1bc29697d71f67541b8b3cec3c7079183b10a83fb98a9ee251d4bac3e1cb581ca972aaed8efd7c2875a6fb4c991132f67c9742d45e53bc7e8eaa94b35b37a907be61086b426cd11088ac118934e85d968c9667fd69fc6f6ea38c0fe34710b7ece91211b9b7ea00acd31f022aa6726368f9928a1352f122233f1":"739df59353ac6694e55e"

generic multi step HMAC-SHA-1 Test Vector NIST CAVS #7
depends_on:MBEDTLS_SHA1_C
md_hmac_multi:"SHA1":10:"1287e1565a57b547":"390ffdccc6171c11568d85b8f913e019bf4cd982ca9cd21ea730d41bdf3fcc0bc88ff48ba13a8f23deb2d96ec1033e7b2a58ca72b0c1e17bf03330db25d1e360fa6918009c4294bd1215b5ccd159a8f58bc3dc3d490eb7c3b9f887e8c98dbbb274a75373dcb695a59abd0219529d88518a96f92abc0bbcbda985c388f1fbbcc9":"d78ddf08077c7d9e2ba6"

generic multi step HMAC-SHA-224 Test Vector NIST CAVS #1
depends_on:MBEDTLS_SHA256_C
md_hmac_multi:"SHA224":14:"e055eb756697ee573fd3214811a9f7fa":"3875847012ee42fe54a0027bdf38cca7021b83a2ed0503af69ef6c37c637bc1114fba40096c5947d736e19b7af3c68d95a4e3b8b073adbbb80f47e9db8f2d4f0018ddd847fabfdf9dd9b52c93e40458977725f6b7ba15f0816bb895cdf50401268f5d702b7e6a5f9faef57b8768c8a3fc14f9a4b3182b41d940e337d219b29ff":"40a453133361cc48da11baf616ee"

generic
multi step HMAC-SHA-224 Test Vector NIST CAVS #2
depends_on:MBEDTLS_SHA256_C
md_hmac_multi:"SHA224":14:"88e5258b55b1623385eb9632fa7c57d6":"ada76bb604be14326551701cf30e48a65eee80b44f0b9d4a07b1844543b7844a621097fdc99de57387458ae9354899b620d0617eabcaefa9eef3d413a33628054335ce656c26fa2986e0f111a6351096b283101ec7868871d770b370973c7405983f9756b3005a3eab492cfd0e7eb42e5c2e15fa6be8718c0a50acc4e5717230":"81c783af538015cef3c60095df53"

generic multi step HMAC-SHA-224 Test Vector NIST CAVS #3
depends_on:MBEDTLS_SHA256_C
md_hmac_multi:"SHA224":14:"85d402d822114d31abf75526e2538705":"8020d8d98cc2e2298b32879c51c751e1dd5558fe2eabb8f158604297d6d072ce2261a1d6830b7cfe2617b57c7126f99c9476211d6161acd75d266da217ec8174b80484c9dc6f0448a0a036a3fc82e8bf54bdb71549368258d5d41f57978a4c266b92e8783ef66350215573d99be4089144b383ad8f3222bae8f3bf80ffb1bb2b":"2aa0340ac9deafe3be38129daca0"

generic
multi step HMAC-SHA-224 Test Vector NIST CAVS #4
depends_on:MBEDTLS_SHA256_C
md_hmac_multi:"SHA224":14:"545c6eecc5ee46fa17c59f91a94f81ae":"8fb7f3565593170152ddb2021874784e951977cfdd22f8b72a72a61320a8f2a35697b5e913f717805559b1af1861ee3ed42fb788481e4fd276b17bdbefcae7b4501dc5

d20de5b7626dd5efdcd65294db4bdf682c33d9a9255c6435383fa5f1c886326a3acbc6bd50a33ab5b2dbb034ce0112d4e226bbcd57e3731a519aa1d784":"3eb566eac54c4a3a9ef092469f24"

generic multi step HMAC-SHA-224 Test Vector NIST CAVS #5
depends_on:MBEDTLS_SHA256_C
md_hmac_multi:"SHA224":14:"4466ab4dc438841a9750c7f173dff02e":"2534c11c78c99cffaec8f722f04adc7045c7324d58ce98e37cfa94b6ed21ed7f58ce55379ef24b72d6d640ee9154f96c614734be9c408e225d7ba4cecc1179cc9f6e1808e1067aa8f244a99bd0c3267594c1887a40d167f8b7cf78db0d19f97b01fc50b8c86def490dfa7a5135002c33e71d77a8cce8ea0f93e0580439a33733":"59f44a9bbed4875b892d22d6b5ab"

generic
multi step HMAC-SHA-224 Test Vector NIST CAVS #6
depends_on:MBEDTLS_SHA256_C
md_hmac_multi:"SHA224":28:"0e3dd9bb5e4cf0f09a4c11600af56d8d":"f4589fa76c328ea25cf8bae582026ba40a59d45a546ff31cf80eb826088f69bb954c452c74586836416dee90a5255bc5d56d3b405b3705a5197045688b32fa984c3a3dfbdc9c2460a0b5e6312a624048bb6f170306535e9b371a3ab134a2642a230ad03d2c688cca80baeaee9a20e1d4c548b1cede29c6a45bf4df2c8c476f1a":"12175b93e3da4c58217145e4dc0a1cf142fab9319bb501e037b350ba"

generic multi step HMAC-SHA-224 Test Vector NIST CAVS #7
depends_on:MBEDTLS_SHA256_C
md_hmac_multi:"SHA224":28:"cda5187b0c5dcb0f8e5a8beed2306584":"9011ae29b44c49b347487ce972965f16ade3c15be0856ce9c853a9739dba07e4f20d594ddc1dfe21560a65a4e458cfa17745575b915a30c7a9412ff8d1d689db9680dd2428c27588bb0dc92d2cd9445fe8f44b840a197c52c3c4333fff45533945134398df6436513cfab06c924046b8c795a5bd92e8d5f2de85bf306f2eed67":"4aaba92b40e2a600feab176eb9b292d814864195c03342aad6f67f08"

generic
multi step HMAC-SHA-256 Test Vector NIST CAVS #1
depends_on:MBEDTLS_SHA256_C
md_hmac_multi:"SHA256":16:"cdffd34e6b16fdc0":"d83e78b99ab61709608972b36e76a575603db742269cc5dd4e7d5ca7816e26b65151c92632550cb4c5253c885d5fce53bc47459a1dbd5652786c4aac0145a532f12c05138af04cbb558101a7af5df478834c2146594dd73690d01a4fe72545894335f427ac70204798068cb86c5a600b40b414ede23590b41e1192373df84fe3":"c6f0dde266cb4a26d41e8259d33499cc"

generic multi step HMAC-SHA-256 Test Vector NIST CAVS #2
depends_on:MBEDTLS_SHA256_C
md_hmac_multi:"SHA256":16:"6d97bb5892245be2":"13c2b391d59c0252ca5d2302beaaf88c4bcd779bb505ad9a122003dfae4cc123ad2bd036f225c4f040021a6b9fb8bd6f0281cf2e2631a732bdc71693cc42ef6d52b6c6912a9ef77b3274eb85ad7f965ae6ed44ac1721962a884ec7acfb4534b1488b1c0c45afa4dae8da1eb7b0a88a3240365d7e4e7d826abbde9f9203fd99d7":"31588e241b015319a5ab8c4527296498"

generic multi step HMAC-SHA-256 Test Vector NIST CAVS #3
depends_on:MBEDTLS_SHA256_C
md_hmac_multi:"SHA256":16:"3c7fc8a70b49007a":"60024e428a39c8b8bb2e9591bad9dc2115dfbfd716b6eb7af30a6eb34560caccbbfa47b710fa8d523aca71e9e5ba10fc1feb1a43556d71f07ea4f33496f093044e8caf1d02b79e46eb1288d5964a7a7494f6b92574c35784eece054c6151281d80822f7d47b8231c35d07f5cb5cf4310ddc844845a01c6bfab514c048eccaf9f":"1c98c94a32bec9f253c21070f82f8438"

generic

multi step HMAC-SHA-256 Test Vector NIST CAVS #4
depends_on:MBEDTLS_SHA256_C
md_hmac_multi:"SHA256":24:"369f33f85b927a07":"ae8e2a94ca386d448cbacdb0e9040ae3cb297c296363052cc15
7455da29a0c95897315fc11e3f12b81e2418da1ec280bccbc00e847584ce9d14deeba7b3c9b8dba958b04bba37551f6c9
ba9c060be1a4b8cf43aa62e5078b76c6512c5619b71a6a7cf5727180e1ff14f5a1a3c1691bf8b6ebad365c151e58d749d
57adb3a4986":"60b90383286533d309de46593e6ce39fc51fb00a8d88278c"

generic multi step HMAC-SHA-256 Test Vector NIST CAVS #5
depends_on:MBEDTLS_SHA256_C
md_hmac_multi:"SHA256":24:"e5179687582b4dc4":"ce103bdacdf32f614f6727bcb31ca1c2824a850d00f5585b016f
b234fe1ef2cd687f302d3c6b738ed89a24060d65c36675d0d96307c72ef3e8a83bfa8402e226de9d5d1724ba75c4879bf
41a4a465ce61887d9f49a34757849b48bae81c27ebed76faae2ad669bca04747d409148d40812776e0ae2c395b3cb9c8
9981ce72d5c":"509581f6816df4b8cc9f2cf42b7cc6e6a5a1e375a16f2412"

generic
multi step HMAC-SHA-256 Test Vector NIST CAVS #6
depends_on:MBEDTLS_SHA256_C
md_hmac_multi:"SHA256":24:"63cec6246aeb1b61":"c178db908a405fa88aa255b8cad22b4057016585f139ee93038
8b083d86062fa0b3ea1f23f8a43bd11bee8464bcbd19b5ab9f6a8038d5245516f8274d20c8ee3033a07b908da528fa003
43bb595deed500cab9745c4cb6391c23300f0d3584b090b3326c4cfa342620b78f9f5b4f27f7307ed770643ec1764aeae
3dcf1a3ec69":"64f3dd861b7c7d29fce9ae0ce9ed954b5d7141806ee9eec7"

generic multi step HMAC-SHA-384 Test Vector NIST CAVS #1
depends_on:MBEDTLS_SHA512_C
md_hmac_multi:"SHA384":32:"91a7401817386948ca952f9a20ee55dc":"2fea5b91035d6d501f3a834fa178bff4e64b
99a8450432dafd32e4466b0e1e7781166f8a73f7e036b3b0870920f559f47bd1400a1a906e85e0dcf00a6c26862e9148b
23806680f285f1fe4f93cdaf924c181a965465739c14f2268c8be8b471847c74b222577a1310bcdc1a85ef1468aa1a3fd4
031213c97324b7509c9050a3d":"6d7be9490058cf413cc09fd043c224c2ec4fa7859b13783000a9a593c9f75838"

generic
multi step HMAC-SHA-384 Test Vector NIST CAVS #2
depends_on:MBEDTLS_SHA512_C
md_hmac_multi:"SHA384":32:"d6cac19657061aa90a6da11cd2e9ea47":"9f482e4655173135dfaa22a11bbbe6af263d
b48716406c5aec162ba3c4b41cad4f5a91558377521191c7343118beee65982929802913d67b6de5c4bdc3d27299bd7
22219d5ad2efa5bdb9ff7b229fc4bbc3f60719320cf2e7a51cad1133d21bad2d80919b1836ef825308b7c51c6b7677ac7
82e2bc30007afba065681cbdd215":"f3d5f3c008175321aa7b2ea379eaa4f8b9dcc60f895ec8940b8162f80a7dfe9f"

generic multi step HMAC-SHA-384 Test Vector NIST CAVS #3
depends_on:MBEDTLS_SHA512_C
md_hmac_multi:"SHA384":32:"e06366ad149b8442cd4c1abdddd0afde":"2d140a194c02a5598f69174834679b8371
234a0d505491f1bd03e128dd91a8bca2fb812e9d5da71613b5b00952ea78bf450d5b7547dea79135925085c7d3e6f520
09c51ca3d88c6c09e9d074b0ee110736e0ec9b478b93efb34d7bf1c41b54decec43eab077a3aa4998ede53f67b4ea36c2
66745f9643d5360bdc8337c70dabf":"c19c67eda6fe29f3667bee1c897c333ce7683094ae77e84b4c16378d290895a1"

generic
multi step HMAC-SHA-384 Test Vector NIST CAVS #4
depends_on:MBEDTLS_SHA512_C
md_hmac_multi:"SHA384":48:"01ac59f42f8bb91d1bd10fe6990d7a87":"3caf18c476edd5615f343ac7b7d3a9da9efa

de755672d5ba4b8ae8a7505539ea2c124ff755ec0457fbe49e43480b3c71e7f4742ec3693aad115d039f90222b030fdc9
440313691716d5302005808c07627483b916fdf61983063c2eb1268f2deeef42fc790334456bc6bad256e31fc9066de7c
c7e43d1321b1866db45e905622":"1985fa2163a5943fc5d92f1fe8831215e7e91f0bff5332bc713a072bdb3a8f9e5c515
7463a3bfeb36231416e65973e64"

generic multi step HMAC-SHA-384 Test Vector NIST CAVS #5
depends_on:MBEDTLS_SHA512_C
md_hmac_multi:"SHA384":48:"fd74b9d9e102a3a80df1baf0cb35bace":"1a068917584813d1689ccbd0370c2114d53
7cdc8cc52bf6db16d5535f8f7d1ad0c850a9fa0cf62373ffbf7642b1f1e8164010d350721d798d9f99e9724830399c2fce
26377e83d38845675457865c03d4a07d741a505ef028343eb29fd46d0f761f3792886998c1e5c32ac3bc7e6f08faed194
b34f06eff4d5d4a5b42c481e0e":"a981eaf5de3d78b20ebd4414a4edd0657e3667cd808a0dbc430cf7252f73a5b24efa1
36039207bd59806897457d74e0c"

generic
multi step HMAC-SHA-384 Test Vector NIST CAVS #5
depends_on:MBEDTLS_SHA512_C
md_hmac_multi:"SHA384":48:"9fe794f0e26b669fa5f6883149377c6c":"6010c9745e8f1d44cfdc99e7e0fd79bc4271
944c2d1d84dba589073dfc4ca5eb98c59356f60cd87bef28aeb83a832bde339b2087daf942aa1f67876c5d5ed33924bed
4143bc12a2be532ccaf64daa7e2bc3c8872b9823b0533b6f5159135effe8c61545536975d7c3a61ba7365ec35f165bc92
b4d19eb9156ade17dfa1bb4161":"915ae61f8754698c2b6ef9629e93441f8541bd4258a5e05372d19136cfaefc0473b48
d96119291b38eb1a3cb1982a986"

generic multi step HMAC-SHA-512 Test Vector NIST CAVS #1
depends_on:MBEDTLS_SHA512_C
md_hmac_multi:"SHA512":32:"c95a17c09940a691ed2d621571b0eb844ede55a9":"99cd28262e81f34878cdcebf412
8e05e2098a7009278a66f4c785784d0e5678f3f2b22f86e982d273b6273a222ec61750b4556d766f1550a7aedfe83faed
bc4bdae83fa560d62df17eb914d05fdaa48940551bac81d700f5fca7147295e386e8120d66742ec65c6ee8d89a92217a0
f6266d0ddc60bb20ef679ae8299c8502c2f":"6bc1379d156559ddee2ed420ea5d5c5ff3e454a1059b7ba72c350e77b6e9
333c"

generic
multi step HMAC-SHA-512 Test Vector NIST CAVS #2
depends_on:MBEDTLS_SHA512_C
md_hmac_multi:"SHA512":32:"3b10b8fa718840d1dea8e9fc317476bcf55875fd":"f04f5b7073d7d0274e8354433b3
90306c5607632f5f589c12edb62d55673aff2366d2e6b24de731adf92e654baa30b1cfd4a069788f65ec1b99b015d904d
8832110dbd74eae35a81562d14ce4136d820ad0a55ff5489ba678fbbc1c27663ec1349d70e740f0e0ec27cfbe8971819f
4789e486b50a2d7271d77e2aaea50de62fd":"fc3c38c7a17e3ce06db033f1c172866f01a00045db55f2e234f71c82264f
2ba2"

generic multi step HMAC-SHA-512 Test Vector NIST CAVS #3
depends_on:MBEDTLS_SHA512_C
md_hmac_multi:"SHA512":32:"4803d311394600dc1e0d8fc8cedeb8bde3fe7c42":"a10c125dd702a97153ad923ba5e
9889cfac1ba169de370debe51f233735aa6effcc9785c4b5c7e48c477dc5c411ae6a959118584e26adc94b42c2b29b046f
3cf01c65b24a24bd2e620bdf650a23bb4a72655b1100d7ce9a4dab697c6379754b4396c825de4b9eb73f2e6a6c0d0353
bbdeaf706612800e137b858fdb30f3311c6":"7cd8236c55102e6385f52279506df6fcc388ab75092da21395ce14a82b2
02ffa"

generic

multi step HMAC-SHA-512 Test Vector NIST CAVS #4
depends_on:MBEDTLS_SHA512_C
md_hmac_multi:"SHA512":48:"aeb2f3b977fa6c8e71e07c5a5c74ff58166de092":"22457355dc76095abd46846b41cf
e49a06ce42ac8857b4702fc771508dfb3626e0bfe851df897a07b36811ec433766e4b4166c26301b3493e7440d4554b0
ef6ac20f1a530e58fac8aeba4e9ff2d4898d8a28783b49cd269c2965fd7f8e4f2d60cf1e5284f2495145b72382aad90e153
a90ecae125ad75336fb128825c23fb8b0":"fa39bd8fcc3bfa218f9dea5d3b2ce10a7619e31678a56d8a9d927b1fe703b1
25af445debe9a89a07db6194d27b44d85a"

generic multi step HMAC-SHA-512 Test Vector NIST CAVS #5
depends_on:MBEDTLS_SHA512_C
md_hmac_multi:"SHA512":48:"4285d3d7744da52775bb44ca436a3154f7980309":"208f0b6f2de2e5aa5df11927ddc
6df485edc1193181c484d0f0a434a95418803101d4de9fdb798f93516a6916fa38a8207de1666fe50fe3441c03b112eaa
ae6954ed063f7ac4e3c1e3f73b20d153fe9e4857f5e91430f0a70ee820529adac2467469fd18adf10e2af0fea27c0abc83c
5a9af77c364a466cffce8bab4e2b70bc1":"fe7603f205b2774fe0f14ecfa3e338e90608a806d11ca459dff5ce36b1b264ec
d3af5f0492a7521d8da3102ba20927a5"

generic
multi step HMAC-SHA-512 Test Vector NIST CAVS #6
depends_on:MBEDTLS_SHA512_C
md_hmac_multi:"SHA512":48:"8ab783d5acf32efa0d9c0a21abce955e96630d89":"17371e013dce839963d54418e97
be4bd9fa3cb2a368a5220f5aa1b8aaddfa3bdefc91afe7c717244fd2fb640f5cb9d9bf3e25f7f0c8bc758883b89dcdce6d7
49d9672fed222277ece3e84b3ec01b96f70c125fcb3cbee6d19b8ef0873f915f173bdb05d81629ba187cc8ac1934b2f75
952fb7616ae6bd812946df694bd2763af":"9ac7ca8d1aefc166b046e4cf7602ebe181a0e5055474bff5b342106731da0d
7e48e4d87bc0a6f05871574289a1b099f8"

generic SHA-1 Test Vector NIST CAVS #1
depends_on:MBEDTLS_SHA1_C
md_hex:"SHA1":"":"da39a3ee5e6b4b0d3255bfef95601890afd80709"

generic SHA-1 Test Vector NIST CAVS #2
depends_on:MBEDTLS_SHA1_C
md_hex:"SHA1":"a8":"99f2aa95e36f95c2acb0eaf23998f030638f3f15"

generic SHA-1 Test Vector NIST CAVS #3
depends_on:MBEDTLS_SHA1_C
md_hex:"SHA1":"3000":"f944dcd635f9801f7ac90a407fbc479964dec024"

generic SHA-1 Test Vector NIST CAVS #4
depends_on:MBEDTLS_SHA1_C
md_hex:"SHA1":"42749e":"a444319e9b6cc1e8464c511ec0969c37d6bb2619"

generic
SHA-1 Test Vector NIST CAVS #5
depends_on:MBEDTLS_SHA1_C
md_hex:"SHA1":"9fc3fe08":"16a0ff84fcc156fd5d3ca3a744f20a232d172253"

generic SHA-1 Test Vector NIST CAVS #6
depends_on:MBEDTLS_SHA1_C

md_hex:"SHA1":"b5c1c6f1af":"fec9deebfcdedaf66dda525e1be43597a73a1f93"

generic SHA-1 Test Vector NIST CAVS #7
depends_on:MBEDTLS_SHA1_C
md_hex:"SHA1":"ec29561244ede706b6eb30a1c371d74450a105c3f9735f7fa9fe38cf67f304a5736a106e92e17139a6813b1c81a4f3d3fb9546ab4296fa9f722826c066869edacd73b2548035185813e22634a9da44000d95a281ff9f264ecce0a931222162d021cca28db5f3c2aa24945ab1e31cb413ae29810fd794cad5dfaf29ec43cb38d198fe4ae1da2359780221405bd6712a5305da4b1b737fce7cd21c0eb7728d08235a9011":"970111c4e77bcc88cc20459c02b69b4aa8f58217"

generic SHA-1 Test Vector NIST CAVS #8
depends_on:MBEDTLS_SHA1_C
md_hex:"SHA1":"5fc2c3f6a7e79dc94be526e5166a238899d54927ce470018fbfd668fd9dd97cbf64e2c91584d01da63be3cc9fdff8adfefc3ac728e1e335b9cdc87f069172e323d094b47fa1e652afe4d6aa147a9f46fda33cacb65f3aa12234746b9007a8c85fe982afed7815221e43dba553d8fe8a022cdac1b99eeeea359e5a9d2e72e382dffa6d19f359f4f27dc3434cd27daeeda8e38594873398678065fbb23665aba9309d946135da0e4a4afdadff14db18e85e71dd93c3bf9faf7f25c8194c4269b1ee3d9934097ab990025d9c3aaf63d5109f52335dd3959d38ae485050e4bbb6235574fc0102be8f7a306d6e8de6ba6becf80f37415b57f9898a5824e77414197422be3d36a6080":"0423dc76a8791107d14e13f5265b343f24cc0f19"

generic
SHA-1 Test Vector NIST CAVS #9
depends_on:MBEDTLS_SHA1_C
md_hex:"SHA1":"0f865f46a8f3aed2da18482aa09a8f390dc9da07d51d1bd10fe0bf5f3928d5927d08733d32075535a6d1c8ac1b2dc6ba0f2f633dc1af68e3f0fa3d85e6c60cb7b56c239dc1519a007ea536a07b518ecca02a6c31b46b76f021620ef3fc6976804018380e5ab9c558ebfc5cb1c9ed2d974722bf8ab6398f1f2b82fa5083f85c16a5767a3a07271d67743f00850ce8ec428c7f22f1cf01f99895c0c844845b06a06cecb0c6cf83eb55a1d4ebc44c2c13f6f7aa5e0e08abfd84e7864279057abc471ee4a45dbbb5774afa24e51791a0eada11093b88681fe30baa3b2e94113dc63342c51ca5d1a6096d0897b626e42cb91761058008f746f35465465540ad8c6b8b60f7e1461b3ce9e6529625984cb8c7d46f07f735be067588a0117f23e34ff57800e2bbe9a1605fde6087fb15d22c5d3ac47566b8c448b0cee40373e5ba6eaa21abee71366afbb27dbbd300477d70c371e7b8963812f5ed4fb784fb2f3bd1d3afe883cdd47ef32beaea":"6692a71d73e00f27df976bc56df4970650d90e45"

generic
SHA-1 Test Vector NIST CAVS #10
depends_on:MBEDTLS_SHA1_C
md_hex:"SHA1":"8236153781bd2f1b81ffe0def1beb46f5a70191142926651503f1b3bb1016acdb9e7f7acced8dd168226f118ff664a01a8800116fd023587bfba52a2558393476f5fc69ce9c65001f23e70476d2cc81c97ea19caeb194e224339bcb23f77a83feac5096f9b3090c51a6ee6d204b735aa71d7e996d380b80822e4dfd43683af9c7442498cacbea64842dfda238cb099927c6efae07fdf7b23a4e4456e0152b24853fe0d5de4179974b2b9d4a1cdbefcbc01d8d311b5dda059136176ea698ab82acf20dd490be47130b1235cb48f8a6710473cfc923e222d94b582f9ae36d4ca2a32d141b8e8cc36638845fbc499bce17698c3fecae2572dbbd470552430d7ef30c238c2124478f1f780483839b4fb73d63a9460206824a5b6b65315b21e3c2f24c97ee7c0e78faad3df549c7ca8ef241876d9aafe9a309f6da352bec2caaa92ee8dca392899ba67dfed90aef33d41fc2494b765cb3e2422c8e595dabbfaca217757453fb322a13203f425f6073a9903e2dc5818ee1da737afc345f0057744e3a56e1681c949eb12273a3bfc20699e423b96e44bd1ff62e50a848a890809bfe1611c6787d3d741103308f849a790f9c015098286dbacfc34c1718b2c2b77e32194a75dda37954a320fa68764027852855a7e5b5274eb1e2cbcd27161d98b59ad245822015f48af82a45c0ed59be94f9af03d9736048570d6e3ef63b1770bc98dfb77de84b1bb1708d872b625d9ab9b06c18e5dbbf34399391f0f8aa26ec0dac7ff4cb8ec97b52bcb942fa6db2385dcd1b3b9d567aaeb425d567b0ebe267235651a1ed9bf78fd93d3c1dd077fe340bb04b00529c58f45124b717c168d07e9826e33376988bc5cf62845c2009980a4dfa69fbc7e5a0b1bb20a5958ca967aec68eb31dd8fccca9afcd30a26bab26279f1bf6724ff":"11863b483809ef88413ca9b008

4ac4a5390640af"

generic
SHA-224 Test Vector NIST CAVS #1
depends_on:MBEDTLS_SHA256_C
md_hex:"SHA224":"":"d14a028c2a3a2bc9476102bb288234c415a2b01f828ea62ac5b3e42f"

generic SHA-224 Test Vector NIST CAVS #2
depends_on:MBEDTLS_SHA256_C
md_hex:"SHA224":"ff":"e33f9d75e6ae1369dbabf81b96b4591ae46bba30b591a6b6c62542b5"

generic
SHA-224 Test Vector NIST CAVS #3
depends_on:MBEDTLS_SHA256_C
md_hex:"SHA224":"984c":"2fa9df9157d9e027cfbc4c6a9df32e1adc0cbe2328ec2a63c5ae934e"

generic SHA-224 Test Vector NIST CAVS #4
depends_on:MBEDTLS_SHA256_C
md_hex:"SHA224":"50efd0":"b5a9820413c2bf8211fbbf5df1337043b32fa4eafaf61a0c8e9ccede"

generic SHA-224 Test Vector NIST CAVS #5
depends_on:MBEDTLS_SHA256_C
md_hex:"SHA224":"e5e09924":"fd19e74690d291467ce59f077df311638f1c3a46e510d0e49a67062d"

generic SHA-224 Test Vector NIST CAVS #6
depends_on:MBEDTLS_SHA256_C
md_hex:"SHA224":"21ebecb914":"78f4a71c21c694499ce1c7866611b14ace70d905012c356323c7c713"

generic SHA-224 Test Vector NIST CAVS #7
depends_on:MBEDTLS_SHA256_C
md_hex:"SHA224":"fc488947c1a7a589726b15436b4f3d9556262f98fc6422fc5cdf20f0fad7fe427a3491c86d101ffe6
b7514f06268f65b2d269b0f69ad9a97847eff1c16a2438775eb7be6847ccf11cb8b2e8dcd6640b095b49c0693fe3cf4a66
e2d9b7ad68bff14f3ad69abf49d0aba36cbe0535202deb6599a47225ef05beb351335cd7bc0f480d691198c7e71305ffd5
3b39d33242bb79cfd98bfd69e137b5d18b2b89ac9ace01c8dbdcf2533cce3682ecc52118de0c1062ec2126c2e657d6ea3
d9e2398e705d4b0b1f1ceecb266dffc4f31bf42744fb1e938dc22a889919ee1e73f463f7871fed720519e32186264b7ef2
a0e5d9a18e6c95c0781894f77967f048951dec3b4d892a38710b1e3436d3c29088eb8b3da1789c25db3d3bc6c2608120
6e7155d210a89b80ca6ea877c41ff9947c0f25625dcb118294a163501f6239c326661a958fd12da4cd15a899f8b88cc72
3589056eaec5aa04a4cf5dbb6f480f9660423ccf38c486e210707e0fb25e1f126ceb2616f63e147a647dab0af9ebe89d65
458bf636154a46e4cab95f5ee62da2c7974cd14b90d3e4f99f81733e85b3c1d5da2b508d9b90f5eed7eff0d9c7649de62
bee00375454fee4a39576a5bbfdae428e7f8097bdf7797f167686cb68407e49079e4611ff3402b6384ba7b7e522bd2bb1
1ce8fd02ea4c1604d163ac4f6dde50b8b1f593f7edaadeac0868ed97df690200680c25f0f5d85431a529e4f339089dcded
a105e4ee51dead704cdf5a605c55fb055c9b0e86b8ba1b564c0dea3eb790a595cb103cb292268b07c5e59371e1a7ef597
cd4b22977a820694c9f9aeb55d9de3ef62b75d6e656e3336698d960a3787bf8cf5b926a7faeef52ae128bcb5dc9e66d94
b016c7b8e034879171a2d91c381f57e6a815b63b5ee6a6d2ff435b49f14c963966960194430d78f8f87627a67757fb353
2b289550894da6dce4817a4e07f4d56877a1102ffcc8befa5c9f8fca6a4574d93ff70376c8861e0f8108cf907fce77ecb49
728f86f034f80224b9695682e0824462f76cdb1fd1af151337b0d85419047a7aa284791718a4860cd586f7824b95bc83
7b6fd4f9be5aade68456e20356aa4d943dac36bf8b67b9e8f9d01a00fcda74b798bafa746c661b010f75b59904b29d0c8
041504811c4065f82cf2ead58d2f595cbd8bc3e7043f4d94577b373b7cfe16a36fe564f505c03b70cfeb5e5f411c794813

38aa67e86b3f5a2e77c21e454c333ae3da943ab723ab5f4c940395319534a5575f64acba0d0ecc43f60221ed3badf7289
c9b3a7b903a2d6c94e15fa4c310dc4fa7faa0c24f405160a1002dbef20e4105d481db982f7243f79400a6e4cd9753c4b97
32a47575f504b20c328fe9add7f432a4f075829da07b53b695037dc51737d3cd731934df333cd1a53fcf65aa31baa450c
a501a6fae26e322347e618c5a444d92e9fec5a8261ae38b98fee5be77c02cec09ddccd5b3de92036":"1302149d1e197c4
1813b054c942329d420e366530f5517b470e964fe"

generic
SHA-256 Test Vector NIST CAVS #1
depends_on:MBEDTLS_SHA256_C
md_hex:"SHA256":"":"e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855"

generic
SHA-256 Test Vector NIST CAVS #2
depends_on:MBEDTLS_SHA256_C
md_hex:"SHA256":"bd":"68325720aabd7c82f30f554b313d0570c95accbb7dc4b5aae11204c08ffe732b"

generic SHA-256 Test Vector NIST CAVS #3
depends_on:MBEDTLS_SHA256_C
md_hex:"SHA256":"5fd4":"7c4fbf484498d21b487b9d61de8914b2eadaf2698712936d47c3ada2558f6788"

generic SHA-256 Test Vector NIST CAVS #4
depends_on:MBEDTLS_SHA256_C
md_hex:"SHA256":"b0bd69":"4096804221093ddccfbf46831490ea63e9e99414858f8d75ff7f642c7ca61803"

generic SHA-256 Test Vector NIST CAVS #5
depends_on:MBEDTLS_SHA256_C
md_hex:"SHA256":"c98c8e55":"7abc22c0ae5af26ce93dbb94433a0e0b2e119d014f8e7f65bd56c61ccccd9504"

generic SHA-256 Test Vector NIST CAVS #6
depends_on:MBEDTLS_SHA256_C
md_hex:"SHA256":"81a723d966":"7516fb8bb11350df2bf386bc3c33bd0f52cb4c67c6e4745e0488e62c2aea2605"

generic SHA-256 Test Vector NIST CAVS #7
depends_on:MBEDTLS_SHA256_C
md_hex:"SHA256":"8390cf0be07661cc7669aac54ce09a37733a629d45f5d983ef201f9b2d13800e555d9b1097fec3b
783d7a50dcb5e2b644b96a1e9463f177cf34906bf388f366db5c2deee04a30e283f764a97c3b377a034fefc22c259214fa
a99babaff160ab0aaa7e2ccb0ce09c6b32fe08cbc474694375aba703fadbfa31cf685b30a11c57f3cf4edd321e57d3ae6eb
b1133c8260e75b9224fa47a2bb205249add2e2e62f817491482ae152322be0900355cdcc8d42a98f82e961a0dc6f537b
7b410eff105f59673bfb787bf042aa071f7af68d944d27371c64160fe9382772372516c230c1f45c0d6b6cca7f274b394d
a9402d3eafdf733994ec58ab22d71829a98399574d4b5908a447a5a681cb0dd50a31145311d92c22a16de1ead66a5499
f2dceb4cae694772ce90762ef8336afec653aa9b1a1c4820b221136dfce80dce2ba920d88a530c9410d0a4e0358a3a110
52e58dd73b0b179ef8f56fe3b5a2d117a73a0c38a1392b6938e9782e0d86456ee4884e3c39d4d75813f13633bc79baa0
7c0d2d555afbf207f52b7dca126d015aa2b9873b3eb065e90b9b065a5373fe1fb1b20d594327d19fba56cb81e7b669660
5ffa56eba3c27a438697cc21b201fd7e09f18deea1b3ea2f0d1edc02df0e20396a145412cd6b13c32d2e605641c948b71
4aec30c0649dc44143511f35ab0fd5dd64c34d06fe86f3836dfe9edeb7f08cfc3bd40956826356242191f99f53473f32b0
cc0cf9321d6c92a112e8db90b86ee9e87cc32d0343db01e32ce9eb782cb24efbbbeb440fe929e8f2bf8dfb1550a3a2e742
e8b455a3e5730e9e6a7a9824d17acc0f72a7f67eae0f0970f8bde46dcdefaed3047cf807e7f00a42e5fd11d40f5e98533d7
574425b7d2bc3b3845c443008b58980e768e464e17cc6f6b3939eee52f713963d07d8c4abf02448ef0b889c9671e2f8a4

36ddeeffcca7176e9bf9d1005ecd377f2fa67c23ed1f137e60bf46018a8bd613d038e883704fc26e798969df35ec7bbc6a
4fe46d8910bd82fa3cded265d0a3b6d399e4251e4d8233daa21b5812fded6536198ff13aa5a1cd46a5b9a17a4ddc1d9f8
5544d1d1cc16f3df858038c8e071a11a7e157a85a6a8dc47e88d75e7009a8b26fdb73f33a2a70f1e0c259f8f9533b9b8f9
af9288b7274f21baeec78d396f8bacdcc22471207d9b4efccd3fedc5c5a2214ff5e51c553f35e21ae696fe51e8df733a8e0
6f50f419e599e9f9e4b37ce643fc810faaa47989771509d69a110ac916261427026369a21263ac4460fb4f708f8ae28599
856db7cb6a43ac8e03d64a9609807e76c5f312b9d1863bfa304e8953647648b4f4ab0ed995e":"4109cdbec3240ad74cc
6c37f39300f70fede16e21efc77f7865998714aad0b5e"

generic
SHA-384 Test Vector NIST CAVS #1
depends_on:MBEDTLS_SHA512_C
md_hex:"SHA384":"":"38b060a751ac96384cd9327eb1b1e36a21fdb71114be07434c0cc7bf63f6e1da274edebfe76f6
5fbd51ad2f14898b95b"

generic
SHA-384 Test Vector NIST CAVS #2
depends_on:MBEDTLS_SHA512_C
md_hex:"SHA384":"ab":"fb94d5be118865f6fcbc978b825da82cff188faec2f66cb84b2537d74b4938469854b0ca89e6
6fa2e182834736629f3d"

generic SHA-384 Test Vector NIST CAVS #3
depends_on:MBEDTLS_SHA512_C
md_hex:"SHA384":"7c27":"3d80be467df86d63abb9ea1d3f9cb39cd19890e7f2c53a6200bedc5006842b35e820dc4e0
ca90ca9b97ab23ef07080fc"

generic SHA-384 Test Vector NIST CAVS #4
depends_on:MBEDTLS_SHA512_C
md_hex:"SHA384":"31f5ca":"78d54b943421fdf7ba90a7fb9637c2073aa480454bd841d39ff72f4511fc21fb67797b65
2c0c823229342873d3bef955"

generic SHA-384 Test Vector NIST CAVS #5
depends_on:MBEDTLS_SHA512_C
md_hex:"SHA384":"7bdee3f8":"8bdafba0777ee446c3431c2d7b1fbb631089f71d2ca417abc1d230e1aba64ec2f1c187
474a6f4077d372c14ad407f99a"

generic SHA-384 Test Vector NIST CAVS #6
depends_on:MBEDTLS_SHA512_C
md_hex:"SHA384":"8f05604915":"504e414bf1db1060f14c8c799e25b1e0c4dcf1504ebbd129998f0ae283e6de86e0d
3c7e879c73ec3b1836c3ee89c2649"

generic
SHA-384 Test Vector NIST CAVS #7
depends_on:MBEDTLS_SHA512_C
md_hex:"SHA384":"665da6eda214":"4c022f112010908848312f8b8f1072625fd5c105399d562ea1d56130619a7eac
8dfc3748fd05ee37e4b690be9daa9980"

generic SHA-384 Test Vector NIST CAVS #8
depends_on:MBEDTLS_SHA512_C

md_hex:"SHA384":"7f46ce506d593c4ed53c82edeb602037e0485befbee03f7f930fe532d18ff2a3f5fd6076672c8145a
1bf40dd94f7abab47c9ae71c234213d2ad1069c2dac0b0ba15257ae672b8245960ae55bd50315c0097daa3a318745788
d70d14706910809ca6e396237fe4934fa46f9ce782d66606d8bd6b2d283b1160513ce9c24e9f084b97891f99d4cdefc16
9a029e431ca772ba1bba426fce6f01d8e286014e5acc66b799e4db62bd4783322f8a32ff78e0de3957df50ce10871f4e06
80df4e8ca3960af9bc6f4efa8eb3962d18f474eb178c3265cc46b8f2ff5ab1a7449fea297dfcfabfa01f28abbb7289bb354b
691b5664ec6d098af51be19947ec5ba7ebd66380d1141953ba78d4aa5401679fa7b0a44db1981f864d3535c45afe4c61
183d5b0ad51fae71ca07e34240283959f7530a32c70d95a088e501c230059f333b0670825009e7e22103ef22935830df
1fac8ef877f5f3426dd54f7d1128dd871ad9a7d088f94c0e8712013295b8d69ae7623b880978c2d3c6ad26dc478f8dc47
f5c0adcc618665dc3dc205a9071b2f2191e16cac5bd89bb59148fc719633752303aa08e518dbc389f0a5482caaa4c507b
8729a6f3edd061efb39026cecc6399f51971cf7381d605e144a5928c8c2d1ad7467b05da2f202f4f3234e1aff19a0198a2
8685721c3d2d52311c721e3fdcbaf30214cdc3acff8c433880e104fb63f2df7ce69a97857819ba7ac00ac8eae1969764fd
e8f68cf8e0916d7e0c151147d4944f99f42ae50f30e1c79a42d2b6c5188d133d3cbbf69094027b354b295ccd0f7dc5a87
d73638bd98ebfb00383ca0fa69cb8dcb35a12510e5e07ad8789047d0b63841a1bb928737e8b0a0c33254f47aa8bfbe33
41a09c2b76dbcefa67e30df300d34f7b8465c4f869e51b6bcfe6cf68b238359a645036bf7f63f02924e087ce7457e483b6
025a859903cb484574aa3b12cf946f32127d537c33bee3141b5db96d10a148c50ae045f287210757710d6846e04b202f
79e87dd9a56bc6da15f84a77a7f63935e1dee00309cd276a8e7176cb04da6bb0e9009534438732cb42d008008853d38d
19beba46e61006e30f7efd1bc7c2906b024e4ff898a1b58c448d68b43c6ab63f34f85b3ac6aa4475867e51b583844cb23
829f4b30f4bdd817d88e2ef3e7b4fc0a624395b05ec5e8686082b24d29fef2b0d3c29e031d5f94f504b1d3df9361eb5ffb
adb242e66c39a8094cfe62f85f639f3fd65fc8ae0c74a8f4c6e1d070b9183a434c722caaa0225f8bcd68614d6f0738ed62f
8484ec96077d155c08e26c46be262a73e3551698bd70d8d5610cf37c4c306eed04ba6a040a9c3e6d7e15e8acda17f477
c2484cf5c56b813313927be8387b1024f995e98fc87f1029091c01424bdc2b296c2eadb7d25b3e762a2fd0c2dcd1727d
df91db97c5984305265f3695a7f5472f2d72c94d68c27914f14f82aa8dd5fe4e2348b0ca967a3f98626a091552f5d0ffa2
bf10350d23c996256c01fdeffb2c2c612519869f877e4929c6e95ff15040f1485e22ed14119880232fef3b57b3848f15b1
766a5552879df8f06":"cba9e3eb12a6f83db11e8a6ff40d1049854ee094416bc527fea931d8585428a8ed6242ce81f676
9b36e2123a5c23483e"

generic
SHA-512 Test Vector NIST CAVS #1
depends_on:MBEDTLS_SHA512_C
md_hex:"SHA512":"":"cf83e1357eefb8bdf1542850d66d8007d620e4050b5715dc83f4a921d36ce9ce47d0d13c5d85f
2b0ff8318d2877eec2f63b931bd47417a81a538327af927da3e"

generic SHA-512 Test Vector NIST CAVS #2
depends_on:MBEDTLS_SHA512_C
md_hex:"SHA512":"8f":"e4cd2d19931b5aad9c920f45f56f6ce34e3d38c6d319a6e11d0588ab8b838576d6ce6d68eea
7c830de66e2bd96458bfa7aafbcbec981d4ed040498c3dd95f22a"

generic
SHA-512 Test Vector NIST CAVS #3
depends_on:MBEDTLS_SHA512_C
md_hex:"SHA512":"e724":"7dbb520221a70287b23dbcf62bfc1b73136d858e86266732a7fffa875ecaa2c1b8f673b5c
065d360c563a7b9539349f5f59bef8c0c593f9587e3cd50bb26a231"

generic SHA-512 Test Vector NIST CAVS #4
depends_on:MBEDTLS_SHA512_C
md_hex:"SHA512":"de4c90":"33ce98281045a5c4c9df0363d8196f1d7dfcd5ee46ac89776fd8a4344c12f123a66788af
5bd41ceff1941aa5637654b4064c88c14e00465ab79a2fc6c97e1014"

generic SHA-512 Test Vector NIST CAVS #5
depends_on:MBEDTLS_SHA512_C
md_hex:"SHA512":"a801e94b":"dadb1b5a27f9fece8d86adb2a51879beb1787ff28f4e8ce162cad7fee0f942efcabbf738bc6f797fc7cc79a3a75048cd4c82ca0757a324695bfb19a557e56e2f"

generic SHA-512 Test Vector NIST CAVS #6
depends_on:MBEDTLS_SHA512_C
md_hex:"SHA512":"94390d3502":"b6175c4c4cccf69e0ce5f0312010886ea6b34d43673f942ae42483f9cbb7da817de4e11b5d58e25a3d9bd721a22cdffe1c40411cc45df1911fa5506129b69297"

generic
SHA-512 Test Vector NIST CAVS #7
depends_on:MBEDTLS_SHA512_C
md_hex:"SHA512":"49297dd63e5f":"1fcc1e6f6870859d11649f5e5336a9cd16329c029baf04d5a6edf257889a2e9522b497dd656bb402da461307c4ee382e2e89380c8e6e6e7697f1e439f650fa94"

generic SHA-512 Test Vector NIST CAVS #8
depends_on:MBEDTLS_SHA512_C
md_hex:"SHA512":"990d1ae71a62d7bda9bfdaa1762a68d296eee72a4cd946f287a898fbabc002ea941fd8d4d991030b4d27a637cce501a834bb95eab1b7889a3e784c7968e67cbf552006b206b68f76d9191327524fcc251aeb56af483d10b4e0c6c5e599ee8c0fe4faeca8293844a8547c6a9a90d093f2526873a19ad4a5e776794c68c742fb834793d2dfcb7fea46c63af4b70fd11cb6e41834e72ee40edb067b292a794990c288d5007e73f349fb383af6a756b8301ad6e5e0aa8cd614399bb3a452376b1575afa6bdaeaafc286cb064bb91edef97c632b6c1113d107fa93a0905098a105043c2f05397f702514439a08a9e5ddc196100721d45c8fc17d2ed659376f8a00bd5cb9a0860e26d8a29d8d6aaf52de97e9346033d6db501a35dbbaf97c20b830cd2d18c2532f3a59cc497ee64c0e57d8d060e5069b28d86edf1adcf59144b221ce3ddaef134b3124fbc7dd000240eff0f5f5f41e83cd7f5bb37c9ae21953fe302b0f6e8b68fa91c6ab99265c64b2fd9cd4942be04321bb5d6d71932376c6f2f88e02422ba6a5e2cb765df93fd5dd0728c6abdaf03bce22e0678a544e2c3636f741b6f4447ee58a8fc656b43ef817932176adbfc2e04b2c812c273cd6cbfa4098f0be036a34221fa02643f5ee2e0b38135f2a18ecd2f16ebc45f8eb31b8ab967a1567ee016904188910861ca1fa205c7adaa194b286893ffe2f4fbe0384c2aef72a4522aeafd3ebc71f9db71eeeef86c48394a1c86d5b36c352cc33a0a2c800bc99e62fd65b3a2fd69e0b53996ec13d8ce483ce9319efd9a85acefabdb5342226febb83fd1daf4b24265f50c61c6de74077ef89b6fecf9f29a1f871af1e9f89b2d345cda7499bd45c42fa5d195a1e1a6ba84851889e730da3b2b916e96152ae0c92154b49719841db7e7cc707ba8a5d7b101eb4ac7b629bb327817910fff61580b59aab78182d1a2e33473d05b00b170b29e331870826cfe45af206aa7d0246bbd8566ca7cfb2d3c10bfa1db7dd48dd786036469ce7282093d78b5e1a5b0fc81a54c8ed4ceac1e5305305e78284ac276f5d7862727aff246e17addde50c670028d572cbfc0be2e4f8b2eb28fa68ad7b4c6c2a239c460441bfb5ea049f23b08563b4e47729a59e5986a61a6093dbd54f8c36ebe87edae01f251cb060ad1364ce677d7e8d5a4a4ca966a7241cc360bc2acb280e5f9e9c1b032ad6a180a35e0c5180b9d16d026c865b252098cc1d99ba7375ca31c7702c0d943d5e3dd2f6861fa55bd46d94b67ed3e52eccd8dd06d968e01897d6de97ed3058d91dd":"8e4bc6f8b8c60fe4d68c61d9b159c8693c3151c46749af58da228442d927f23359bd6ccd6c2ec8fa3f00a86cecbfa728e1ad60b821ed22fcd309ba91a4138bc9"

generic
multi step SHA-1 Test Vector NIST CAVS #1
depends_on:MBEDTLS_SHA1_C
md_hex_multi:"SHA1":"":"da39a3ee5e6b4b0d3255bfef95601890afd80709"

generic multi step SHA-1 Test Vector NIST CAVS #2
depends_on:MBEDTLS_SHA1_C
md_hex_multi:"SHA1":"a8":"99f2aa95e36f95c2acb0eaf23998f030638f3f15"

generic multi step SHA-1 Test Vector NIST CAVS #3
depends_on:MBEDTLS_SHA1_C
md_hex_multi:"SHA1":"3000":"f944dcd635f9801f7ac90a407fbc479964dec024"

generic multi step SHA-1 Test Vector NIST CAVS #4
depends_on:MBEDTLS_SHA1_C
md_hex_multi:"SHA1":"42749e":"a444319e9b6cc1e8464c511ec0969c37d6bb2619"

generic multi step SHA-1 Test Vector NIST
CAVS #5
depends_on:MBEDTLS_SHA1_C
md_hex_multi:"SHA1":"9fc3fe08":"16a0ff84fcc156fd5d3ca3a744f20a232d172253"

generic multi step SHA-1 Test Vector NIST CAVS #6
depends_on:MBEDTLS_SHA1_C
md_hex_multi:"SHA1":"b5c1c6f1af":"fec9deebfcdedaf66dda525e1be43597a73a1f93"

generic multi step SHA-1 Test Vector NIST CAVS #7
depends_on:MBEDTLS_SHA1_C
md_hex_multi:"SHA1":"ec29561244ede706b6eb30a1c371d74450a105c3f9735f7fa9fe38cf67f304a5736a106e92e17139a6813b1c81a4f3d3fb9546ab4296fa9f722826c066869edacd73b2548035185813e22634a9da44000d95a281ff9f264ecce0a931222162d021cca28db5f3c2aa24945ab1e31cb413ae29810fd794cad5dfaf29ec43cb38d198fe4ae1da2359780221405bd6712a5305da4b1b737fce7cd21c0eb7728d08235a9011":"970111c4e77bcc88cc20459c02b69b4aa8f58217"

generic multi step SHA-1 Test Vector NIST CAVS #8
depends_on:MBEDTLS_SHA1_C
md_hex_multi:"SHA1":"5fc2c3f6a7e79dc94be526e5166a238899d54927ce470018fbfd668fd9dd97cbf64e2c91584d01da63be3cc9fdff8adfefc3ac728e1e335b9cdc87f069172e323d094b47fa1e652afe4d6aa147a9f46fda33cacb65f3aa12234746b9007a8c85fe982afed7815221e43dba553d8fe8a022cdac1b99eeeea359e5a9d2e72e382dffa6d19f359f4f27dc3434cd27daeeda8e38594873398678065fbb23665aba9309d946135da0e4a4afdadff14db18e85e71dd93c3bf9faf7f25c8194c4269b1ee3d9934097ab990025d9c3aaf63d5109f52335dd3959d38ae485050e4bbb6235574fc0102be8f7a306d6e8de6ba6becf80f37415b57f9898a5824e77414197422be3d36a6080":"0423dc76a8791107d14e13f5265b343f24cc0f19"

generic
multi step SHA-1 Test Vector NIST CAVS #9
depends_on:MBEDTLS_SHA1_C
md_hex_multi:"SHA1":"0f865f46a8f3aed2da18482aa09a8f390dc9da07d51d1bd10fe0bf5f3928d5927d08733d32075535a6d1c8ac1b2dc6ba0f2f633dc1af68e3f0fa3d85e6c60cb7b56c239dc1519a007ea536a07b518ecca02a6c31b46b76f021620ef3fc6976804018380e5ab9c558ebfc5cb1c9ed2d974722bf8ab6398f1f2b82fa5083f85c16a5767a3a07271d67743f00850ce8ec428c7f22f1cf01f99895c0c844845b06a06cecb0c6cf83eb55a1d4ebc44c2c13f6f7aa5e0e08abfd84e7864279057abc471ee4a45dbbb5774afa24e51791a0eada11093b88681fe30baa3b2e94113dc63342c51ca5d1a6096d0897b626e42cb91761058008f746f35465465540ad8c6b8b60f7e1461b3ce9e6529625984cb8c7d46f07f735be067588a0117f23e34ff57800e2bbe9a1605fde6087fb15d22c5d3ac47566b8c448b0cee40373e5ba6eaa21abee71366afbb27dbbd300477d70c371e7b8963812f5ed4fb784fb2f3bd1d3afe883cdd47ef32beaea":"6692a71d73e00f27df976bc56df4970650d90e45"

generic
 multi step SHA-1 Test Vector NIST CAVS #10
depends_on:MBEDTLS_SHA1_C
md_hex_multi:"SHA1":"8236153781bd2f1b81ffe0def1beb46f5a70191142926651503f1b3bb1016acdb9e7f7acced8
dd168226f118ff664a01a8800116fd023587bfba52a2558393476f5fc69ce9c65001f23e70476d2cc81c97ea19caeb194e
224339bcb23f77a83feac5096f9b3090c51a6ee6d204b735aa71d7e996d380b80822e4dfd43683af9c7442498cacbea64
842dfda238cb099927c6efae07fdf7b23a4e4456e0152b24853fe0d5de4179974b2b9d4a1cdbefcbc01d8d311b5dda059
136176ea698ab82acf20dd490be47130b1235cb48f8a6710473cfc923e222d94b582f9ae36d4ca2a32d141b8e8cc36638
845fbc499bce17698c3fecae2572dbbd470552430d7ef30c238c2124478f1f780483839b4fb73d63a9460206824a5b6b6
5315b21e3c2f24c97ee7c0e78faad3df549c7ca8ef241876d9aafe9a309f6da352bec2caaa92ee8dca392899ba67dfed90a
ef33d41fc2494b765cb3e2422c8e595dabbfaca217757453fb322a13203f425f6073a9903e2dc5818ee1da737afc345f00
57744e3a56e1681c949eb12273a3bfc20699e423b96e44bd1ff62e50a848a890809bfe1611c6787d3d741103308f849a
790f9c015098286dbacfc34c1718b2c2b77e32194a75dda37954a320fa68764027852855a7e5b5274eb1e2cbcd27161d
98b59ad245822015f48af82a45c0ed59be94f9af03d9736048570d6e3ef63b1770bc98dfb77de84b1bb1708d872b625d
9ab9b06c18e5dbbf34399391f0f8aa26ec0dac7ff4cb8ec97b52bcb942fa6db2385dcd1b3b9d567aaeb425d567b0ebe26
7235651a1ed9bf78fd93d3c1dd077fe340bb04b00529c58f45124b717c168d07e9826e33376988bc5cf62845c2009980
a4dfa69fbc7e5a0b1bb20a5958ca967aec68eb31dd8fccca9afcd30a26bab26279f1bf6724ff":"11863b483809ef88413c
a9b0084ac4a5390640af"

generic
 multi step SHA-224 Test Vector NIST CAVS #1
depends_on:MBEDTLS_SHA256_C
md_hex_multi:"SHA224":"":"d14a028c2a3a2bc9476102bb288234c415a2b01f828ea62ac5b3e42f"

generic multi step SHA-224 Test Vector NIST CAVS #2
depends_on:MBEDTLS_SHA256_C
md_hex_multi:"SHA224":"ff":"e33f9d75e6ae1369dbabf81b96b4591ae46bba30b591a6b6c62542b5"

generic
 multi step SHA-224 Test Vector NIST CAVS #3
depends_on:MBEDTLS_SHA256_C
md_hex_multi:"SHA224":"984c":"2fa9df9157d9e027cfbc4c6a9df32e1adc0cbe2328ec2a63c5ae934e"

generic multi step SHA-224 Test Vector NIST CAVS #4
depends_on:MBEDTLS_SHA256_C
md_hex_multi:"SHA224":"50efd0":"b5a9820413c2bf8211fbbf5df1337043b32fa4eafaf61a0c8e9ccede"

generic multi step SHA-224 Test Vector NIST CAVS #5
depends_on:MBEDTLS_SHA256_C
md_hex_multi:"SHA224":"e5e09924":"fd19e74690d291467ce59f077df311638f1c3a46e510d0e49a67062d"

generic multi step SHA-224 Test Vector NIST CAVS #6
depends_on:MBEDTLS_SHA256_C
md_hex_multi:"SHA224":"21ebecb914":"78f4a71c21c694499ce1c7866611b14ace70d905012c356323c7c713"

generic multi step SHA-224 Test Vector NIST CAVS #7
depends_on:MBEDTLS_SHA256_C

md_hex_multi:"SHA224":"fc488947c1a7a589726b15436b4f3d9556262f98fc6422fc5cdf20f0fad7fe427a3491c86d1
01ffe6b7514f06268f65b2d269b0f69ad9a97847eff1c16a2438775eb7be6847ccf11cb8b2e8dcd6640b095b49c0693fe3
cf4a66e2d9b7ad68bff14f3ad69abf49d0aba36cbe0535202deb6599a47225ef05beb351335cd7bc0f480d691198c7e71
305ffd53b39d33242bb79cfd98bfd69e137b5d18b2b89ac9ace01c8dbdcf2533cce3682ecc52118de0c1062ec2126c2e6
57d6ea3d9e2398e705d4b0b1f1ceecb266dffc4f31bf42744fb1e938dc22a889919ee1e73f463f7871fed720519e321862
64b7ef2a0e5d9a18e6c95c0781894f77967f048951dec3b4d892a38710b1e3436d3c29088eb8b3da1789c25db3d3bc6c
26081206e7155d210a89b80ca6ea877c41ff9947c0f25625dcb118294a163501f6239c326661a958fd12da4cd15a899f8
b88cc723589056eaec5aa04a4cf5dbb6f480f9660423ccf38c486e210707e0fb25e1f126ceb2616f63e147a647dab0af9e
be89d65458bf636154a46e4cab95f5ee62da2c7974cd14b90d3e4f99f81733e85b3c1d5da2b508d9b90f5eed7eff0d9c7
649de62bee00375454fee4a39576a5bbfdae428e7f8097bdf7797f167686cb68407e49079e4611ff3402b6384ba7b7e52
2bd2bb11ce8fd02ea4c1604d163ac4f6dde50b8b1f593f7edaadeac0868ed97df690200680c25f0f5d85431a529e4f3390
89dcdeda105e4ee51dead704cdf5a605c55fb055c9b0e86b8ba1b564c0dea3eb790a595cb103cb292268b07c5e59371e
1a7ef597cd4b22977a820694c9f9aeb55d9de3ef62b75d6e656e3336698d960a3787bf8cf5b926a7faeef52ae128bcb5dc
9e66d94b016c7b8e034879171a2d91c381f57e6a815b63b5ee6a6d2ff435b49f14c963966960194430d78f8f87627a67
757fb3532b289550894da6dce4817a4e07f4d56877a1102ffcc8befa5c9f8fca6a4574d93ff70376c8861e0f8108cf907fc
e77ecb49728f86f034f80224b9695682e0824462f76cdb1fd1af151337b0d85419047a7aa284791718a4860cd586f7824
b95bc837b6fd4f9be5aade68456e20356aa4d943dac36bf8b67b9e8f9d01a00fcda74b798bafa746c661b010f75b59904
b29d0c8041504811c4065f82cf2ead58d2f595cbd8bc3e7043f4d94577b373b7cfe16a36fe564f505c03b70cfeb5e5f411
c79481338aa67e86b3f5a2e77c21e454c333ae3da943ab723ab5f4c940395319534a5575f64acba0d0ecc43f60221ed3b
adf7289c9b3a7b903a2d6c94e15fa4c310dc4fa7faa0c24f405160a1002dbef20e4105d481db982f7243f79400a6e4cd97
53c4b9732a47575f504b20c328fe9add7f432a4f075829da07b53b695037dc51737d3cd731934df333cd1a53fcf65aa31
baa450ca501a6fae26e322347e618c5a444d92e9fec5a8261ae38b98fee5be77c02cec09ddccd5b3de92036":"1302149d
1e197c41813b054c942329d420e366530f5517b470e964fe"

generic
multi step SHA-256 Test Vector NIST CAVS #1
depends_on:MBEDTLS_SHA256_C
md_hex_multi:"SHA256":"":"e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855"

generic multi step SHA-256 Test Vector NIST CAVS #2
depends_on:MBEDTLS_SHA256_C
md_hex_multi:"SHA256":"bd":"68325720aabd7c82f30f554b313d0570c95accbb7dc4b5aae11204c08ffe732b"

generic multi step SHA-256 Test Vector NIST CAVS #3
depends_on:MBEDTLS_SHA256_C
md_hex_multi:"SHA256":"5fd4":"7c4fbf484498d21b487b9d61de8914b2eadaf2698712936d47c3ada2558f6788"

generic multi step SHA-256 Test Vector NIST CAVS #4
depends_on:MBEDTLS_SHA256_C
md_hex_multi:"SHA256":"b0bd69":"4096804221093ddccfbf46831490ea63e9e99414858f8d75ff7f642c7ca61803"

generic multi step SHA-256 Test Vector NIST CAVS #5
depends_on:MBEDTLS_SHA256_C
md_hex_multi:"SHA256":"c98c8e55":"7abc22c0ae5af26ce93dbb94433a0e0b2e119d014f8e7f65bd56c61ccccd9504
"

generic multi step SHA-256 Test Vector NIST CAVS #6
depends_on:MBEDTLS_SHA256_C

md_hex_multi:"SHA256":"81a723d966":"7516fb8bb11350df2bf386bc3c33bd0f52cb4c67c6e4745e0488e62c2aea2605"

generic
multi step SHA-256 Test Vector NIST CAVS #7
depends_on:MBEDTLS_SHA256_C
md_hex_multi:"SHA256":"8390cf0be07661cc7669aac54ce09a37733a629d45f5d983ef201f9b2d13800e555d9b1097fec3b783d7a50dcb5e2b644b96a1e9463f177cf34906bf388f366db5c2deee04a30e283f764a97c3b377a034fefc22c259214faa99babaff160ab0aaa7e2ccb0ce09c6b32fe08cbc474694375aba703fadbfa31cf685b30a11c57f3cf4edd321e57d3ae6ebb1133c8260e75b9224fa47a2bb205249add2e2e62f817491482ae152322be0900355cdcc8d42a98f82e961a0dc6f537b7b410eff105f59673bfb787bf042aa071f7af68d944d27371c64160fe9382772372516c230c1f45c0d6b6cca7f274b394da9402d3eafdf733994ec58ab22d71829a98399574d4b5908a447a5a681cb0dd50a31145311d92c22a16de1ead66a5499f2dceb4cae694772ce90762ef8336afec653aa9b1a1c4820b221136dfce80dce2ba920d88a530c9410d0a4e0358a3a11052e58dd73b0b179ef8f56fe3b5a2d117a73a0c38a1392b6938e9782e0d86456ee4884e3c39d4d75813f13633bc79baa07c0d2d555afbf207f52b7dca126d015aa2b9873b3eb065e90b9b065a5373fe1fb1b20d594327d19fba56cb81e7b6696605ffa56eba3c27a438697cc21b201fd7e09f18deea1b3ea2f0d1edc02df0e20396a145412cd6b13c32d2e605641c948b714aec30c0649dc44143511f35ab0fd5dd64c34d06fe86f3836dfe9edeb7f08cfc3bd4095682635624219 1f99f53473f32b0cc0cf9321d6c92a112e8db90b86ee9e87cc32d0343db01e32ce9eb782cb24efbbbeb440fe929e8f2bf8dfb1550a3a2e742e8b455a3e5730e9e6a7a9824d17acc0f72a7f67eae0f0970f8bde46dcdefaed3047cf807e7f00a42e5fd11d40f5e98533d7574425b7d2bc3b3845c443008b58980e768e464e17cc6f6b3939eee52f713963d07d8c4abf02448ef0b889c9671e2f8a436ddeeffcca7176e9bf9d1005ecd377f2fa67c23ed1f137e60bf46018a8bd613d038e883704fc26e798969df35ec7bbc6a4fe46d8910bd82fa3cded265d0a3b6d399e4251e4d8233daa21b5812fded6536198ff13aa5a1cd46a5b9a17a4ddc1d9f85544d1d1cc16f3df858038c8e071a11a7e157a85a6a8dc47e88d75e7009a8b26fdb73f33a2a70f1e0c259f8f9533b9b8f9af9288b7274f21baeec78d396f8bacdcc22471207d9b4efccd3fedc5c5a2214ff5e51c553f35e21ae696fe51e8df733a8e06f50f419e599e9f9e4b37ce643fc810faaa47989771509d69a110ac916261427026369a21263ac4460fb4f708f8ae28599856db7cb6a43ac8e03d64a9609807e76c5f312b9d1863bfa304e8953647648b4f4ab0ed995e":"4109cdbec3240ad74cc6c37f39300f70fede16e21efc77f7865998714aad0b5e"

generic
multi step SHA-384 Test Vector NIST CAVS #1
depends_on:MBEDTLS_SHA512_C
md_hex_multi:"SHA384":"":"38b060a751ac96384cd9327eb1b1e36a21fdb71114be07434c0cc7bf63f6e1da274edebfe76f65fbd51ad2f14898b95b"

generic multi step SHA-384 Test Vector NIST CAVS #2
depends_on:MBEDTLS_SHA512_C
md_hex_multi:"SHA384":"ab":"fb94d5be118865f6fcbc978b825da82cff188faec2f66cb84b2537d74b4938469854b0ca89e66fa2e182834736629f3d"

generic multi step SHA-384 Test Vector NIST CAVS #3
depends_on:MBEDTLS_SHA512_C
md_hex_multi:"SHA384":"7c27":"3d80be467df86d63abb9ea1d3f9cb39cd19890e7f2c53a6200bedc5006842b35e820dc4e0ca90ca9b97ab23ef07080fc"

generic multi step SHA-384 Test Vector NIST CAVS #4
depends_on:MBEDTLS_SHA512_C
md_hex_multi:"SHA384":"31f5ca":"78d54b943421fdf7ba90a7fb9637c2073aa480454bd841d39ff72f4511fc21fb67797b652c0c823229342873d3bef955"

generic
multi step SHA-384 Test Vector NIST CAVS #5
depends_on:MBEDTLS_SHA512_C
md_hex_multi:"SHA384":"7bdee3f8":"8bdafba0777ee446c3431c2d7b1fbb631089f71d2ca417abc1d230e1aba64ec2f1c187474a6f4077d372c14ad407f99a"

generic multi step SHA-384 Test Vector NIST CAVS #6
depends_on:MBEDTLS_SHA512_C
md_hex_multi:"SHA384":"8f05604915":"504e414bf1db1060f14c8c799e25b1e0c4dcf1504ebbd129998f0ae283e6de86e0d3c7e879c73ec3b1836c3ee89c2649"

generic multi step SHA-384 Test Vector NIST CAVS #7
depends_on:MBEDTLS_SHA512_C
md_hex_multi:"SHA384":"665da6eda214":"4c022f112010908848312f8b8f1072625fd5c105399d562ea1d56130619a7eac8dfc3748fd05ee37e4b690be9daa9980"

generic multi step SHA-384 Test Vector NIST CAVS #8
depends_on:MBEDTLS_SHA512_C
md_hex_multi:"SHA384":"7f46ce506d593c4ed53c82edeb602037e0485befbee03f7f930fe532d18ff2a3f5fd6076672c8145a1bf40dd94f7abab47c9ae71c234213d2ad1069c2dac0b0ba15257ae672b8245960ae55bd50315c0097daa3a318745788d70d14706910809ca6e396237fe4934fa46f9ce782d66606d8bd6b2d283b1160513ce9c24e9f084b97891f99d4cdefc169a029e431ca772ba1bba426fce6f01d8e286014e5acc66b799e4db62bd4783322f8a32ff78e0de3957df50ce10871f4e0680df4e8ca3960af9bc6f4efa8eb3962d18f474eb178c3265cc46b8f2ff5ab1a7449fea297dfcfabfa01f28abbb7289bb354b691b5664ec6d098af51be19947ec5ba7ebd66380d1141953ba78d4aa5401679fa7b0a44db1981f864d3535c45afe4c61183d5b0ad51fae71ca07e34240283959f7530a32c70d95a088e501c230059f333b0670825009e7e22103ef22935830df1fac8ef877f5f3426dd54f7d1128dd871ad9a7d088f94c0e8712013295b8d69ae7623b880978c2d3c6ad26dc478f8dc47f5c0adcc618665dc3dc205a9071b2f2191e16cac5bd89bb59148fc719633752303aa08e518dbc389f0a5482caaa4c507b8729a6f3edd061efb39026cecc6399f51971cf7381d605e144a5928c8c2d1ad7467b05da2f202f4f3234e1aff19a0198a28685721c3d2d52311c721e3fdcbaf30214cdc3acff8c433880e104fb63f2df7ce69a97857819ba7ac00ac8eae1969764fde8f68cf8e0916d7e0c151147d4944f99f42ae50f30e1c79a42d2b6c5188d133d3cbbf69094027b354b295ccd0f7dc5a87d73638bd98ebfb00383ca0fa69cb8dcb35a12510e5e07ad8789047d0b63841a1bb928737e8b0a0c33254f47aa8bfbe3341a09c2b76dbcefa67e30df300d34f7b8465c4f869e51b6bcfe6cf68b238359a645036bf7f63f02924e087ce7457e483b6025a859903cb484574aa3b12cf946f32127d537c33bee3141b5db96d10a148c50ae045f287210757710d6846e04b202f79e87dd9a56bc6da15f84a77a7f63935e1dee00309cd276a8e7176cb04da6bb0e9009534438732cb42d008008853d38d19beba46e61006e30f7efd1bc7c2906b024e4ff898a1b58c448d68b43c6ab63f34f85b3ac6aa4475867e51b583844cb23829f4b30f4bdd817d88e2ef3e7b4fc0a624395b05ec5e8686082b24d29fef2b0d3c29e031d5f94f504b1d3df9361eb5ffbadb242e66c39a8094cfe62f85f639f3fd65fc8ae0c74a8f4c6e1d070b9183a434c722caaa0225f8bcd68614d6f0738ed62f8484ec96077d155c08e26c46be262a73e3551698bd70d8d5610cf37c4c306eed04ba6a040a9c3e6d7e15e8acda17f477c2484cf5c56b813313927be8387b1024f995e98fc87f1029091c01424bdc2b296c2eadb7d25b3e762a2fd0c2dcd1727ddf91db97c5984305265f3695a7f5472f2d72c94d68c27914f14f82aa8dd5fe4e2348b0ca967a3f98626a091552f5d0ffa2bf10350d23c996256c01fdeffb2c2c612519869f877e4929c6e95ff15040f1485e22ed14119880232fef3b57b3848f15b1766a5552879df8f06":"cba9e3eb12a6f83db11e8a6ff40d1049854ee094416bc527fea931d8585428a8ed6242ce81f6769b36e2123a5c23483e"

generic
multi step SHA-512 Test Vector NIST CAVS #1
depends_on:MBEDTLS_SHA512_C

md_hex_multi:"SHA512":"":"cf83e1357eefb8bdf1542850d66d8007d620e4050b5715dc83f4a921d36ce9ce47d0d13c5d85f2b0ff8318d2877eec2f63b931bd47417a81a538327af927da3e"

generic multi step SHA-512 Test Vector NIST CAVS #2
depends_on:MBEDTLS_SHA512_C
md_hex_multi:"SHA512":"8f":"e4cd2d19931b5aad9c920f45f56f6ce34e3d38c6d319a6e11d0588ab8b838576d6ce6d68eea7c830de66e2bd96458bfa7aafbcbec981d4ed040498c3dd95f22a"

generic multi step SHA-512 Test Vector NIST CAVS #3
depends_on:MBEDTLS_SHA512_C
md_hex_multi:"SHA512":"e724":"7dbb520221a70287b23dbcf62bfc1b73136d858e86266732a7fffa875ecaa2c1b8f673b5c065d360c563a7b9539349f5f59bef8c0c593f9587e3cd50bb26a231"

generic multi step SHA-512 Test Vector NIST CAVS #4
depends_on:MBEDTLS_SHA512_C
md_hex_multi:"SHA512":"de4c90":"33ce98281045a5c4c9df0363d8196f1d7dfcd5ee46ac89776fd8a4344c12f123a66788af5bd41ceff1941aa5637654b4064c88c14e00465ab79a2fc6c97e1014"

generic
multi step SHA-512 Test Vector NIST CAVS #5
depends_on:MBEDTLS_SHA512_C
md_hex_multi:"SHA512":"a801e94b":"dadb1b5a27f9fece8d86adb2a51879beb1787ff28f4e8ce162cad7fee0f942efcabbf738bc6f797fc7cc79a3a75048cd4c82ca0757a324695bfb19a557e56e2f"

generic multi step SHA-512 Test Vector NIST CAVS #6
depends_on:MBEDTLS_SHA512_C
md_hex_multi:"SHA512":"94390d3502":"b6175c4c4cccf69e0ce5f0312010886ea6b34d43673f942ae42483f9cbb7da817de4e11b5d58e25a3d9bd721a22cdffe1c40411cc45df1911fa5506129b69297"

generic multi step SHA-512 Test Vector NIST CAVS #7
depends_on:MBEDTLS_SHA512_C
md_hex_multi:"SHA512":"49297dd63e5f":"1fcc1e6f6870859d11649f5e5336a9cd16329c029baf04d5a6edf257889a2e9522b497dd656bb402da461307c4ee382e2e89380c8e6e6e7697f1e439f650fa94"

generic multi step SHA-512 Test Vector NIST CAVS #8
depends_on:MBEDTLS_SHA512_C
md_hex_multi:"SHA512":"990d1ae71a62d7bda9bfdaa1762a68d296eee72a4cd946f287a898fbabc002ea941fd8d4d991030b4d27a637cce501a834bb95eab1b7889a3e784c7968e67cbf552006b206b68f76d9191327524fcc251aeb56af483d10b4e0c6c5e599ee8c0fe4faeca8293844a8547c6a9a90d093f2526873a19ad4a5e776794c68c742fb834793d2dfcb7fea46c63af4b70fd11cb6e41834e72ee40edb067b292a794990c288d5007e73f349fb383af6a756b8301ad6e5e0aa8cd614399bb3a452376b1575afa6bdaeaafc286cb064bb91edef97c632b6c1113d107fa93a0905098a105043c2f05397f702514439a08a9e5ddc196100721d45c8fc17d2ed659376f8a00bd5cb9a0860e26d8a29d8d6aaf52de97e9346033d6db501a35dbbaf97c20b830cd2d18c2532f3a59cc497ee64c0e57d8d060e5069b28d86edf1adcf59144b221ce3ddaef134b3124fbc7dd000240eff0f5f5f41e83cd7f5bb37c9ae21953fe302b0f6e8b68fa91c6ab99265c64b2fd9cd4942be04321bb5d6d71932376c6f2f88e02422ba6a5e2cb765df93fd5dd0728c6abdaf03bce22e0678a544e2c3636f741b6f4447ee58a8fc656b43ef817932176adbfc2e04b2c812c273cd6cbfa4098f0be036a34221fa02643f5ee2e0b38135f2a18ecd2f16ebc45f8eb31b8ab967a1567ee016904188910861ca1fa205c7adaa194b286893ffe2f4fbe0384c2aef72a4522aeafd3ebc71f9db71eeeef86c48394a1c86d5b36c352cc33a0a2c800bc99e62fd65b3a2fd69e0b53996ec13d8ce483ce9319efd9a85acefabdb5342

226febb83fd1daf4b24265f50c61c6de74077ef89b6fecf9f29a1f871af1e9f89b2d345cda7499bd45c42fa5d195a1e1a6b
a84851889e730da3b2b916e96152ae0c92154b49719841db7e7cc707ba8a5d7b101eb4ac7b629bb327817910fff61580
b59aab78182d1a2e33473d05b00b170b29e331870826cfe45af206aa7d0246bbd8566ca7cfb2d3c10bfa1db7dd48dd78
6036469ce7282093d78b5e1a5b0fc81a54c8ed4ceac1e5305305e78284ac276f5d7862727aff246e17addde50c670028d
572cbfc0be2e4f8b2eb28fa68ad7b4c6c2a239c460441bfb5ea049f23b08563b4e47729a59e5986a61a6093dbd54f8c36
ebe87edae01f251cb060ad1364ce677d7e8d5a4a4ca966a7241cc360bc2acb280e5f9e9c1b032ad6a180a35e0c5180b9d
16d026c865b252098cc1d99ba7375ca31c7702c0d943d5e3dd2f6861fa55bd46d94b67ed3e52eccd8dd06d968e01897d
6de97ed3058d91dd":"8e4bc6f8b8c60fe4d68c61d9b159c8693c3151c46749af58da228442d927f23359bd6ccd6c2ec8
fa3f00a86cecbfa728e1ad60b821ed22fcd309ba91a4138bc9"

generic
SHA1 Hash file #1
depends_on:MBEDTLS_SHA1_C
mbedtls_md_file:"SHA1":"data_files/hash_file_1":"d21c965b1e768bd7a6aa6869f5f821901d255f9f"

generic
SHA1 Hash file #2
depends_on:MBEDTLS_SHA1_C
mbedtls_md_file:"SHA1":"data_files/hash_file_2":"353f34271f2aef49d23a8913d4a6bd82b2cecdc6"

generic SHA1 Hash file #3
depends_on:MBEDTLS_SHA1_C
mbedtls_md_file:"SHA1":"data_files/hash_file_3":"93640ed592076328096270c756db2fba9c486b35"

generic SHA1 Hash file #4
depends_on:MBEDTLS_SHA1_C
mbedtls_md_file:"SHA1":"data_files/hash_file_4":"da39a3ee5e6b4b0d3255bfef95601890afd80709"

generic SHA-224 Hash file #1
depends_on:MBEDTLS_SHA256_C
mbedtls_md_file:"SHA224":"data_files/hash_file_1":"8606da018870f0c16834a21bc3385704cb1683b9dbab04c5dd
b90a48"

generic SHA-224 Hash file #2
depends_on:MBEDTLS_SHA256_C
mbedtls_md_file:"SHA224":"data_files/hash_file_2":"733b2ab97b6f63f2e29b9a2089756d81e14c93fe4cc9615c0d5
e8a03"

generic SHA-224 Hash file #3
depends_on:MBEDTLS_SHA256_C
mbedtls_md_file:"SHA224":"data_files/hash_file_3":"e1df95867580e2cc2100e9565bf9c2e42c24fe5250c19efe33d1
c4fe"

generic SHA-224 Hash file #4
depends_on:MBEDTLS_SHA256_C
mbedtls_md_file:"SHA224":"data_files/hash_file_4":"d14a028c2a3a2bc9476102bb288234c415a2b01f828ea62ac5b
3e42f"

generic
SHA-256 Hash file #1
depends_on:MBEDTLS_SHA256_C
mbedtls_md_file:"SHA256":"data_files/hash_file_1":"975d0c620d3936886f8a3665e585a3e84aa0501f4225bf53029710242823e391"

generic SHA-256 Hash file #2
depends_on:MBEDTLS_SHA256_C
mbedtls_md_file:"SHA256":"data_files/hash_file_2":"11fcbf1baa36ca45745f10cc5467aee86f066f80ba2c46806d876bf783022ad2"

generic SHA-256 Hash file #3
depends_on:MBEDTLS_SHA256_C
mbedtls_md_file:"SHA256":"data_files/hash_file_3":"9ae4b369f9f4f03b86505b46a5469542e00aaff7cf7417a71af6d6d0aba3b70c"

generic SHA-256 Hash file #4
depends_on:MBEDTLS_SHA256_C
mbedtls_md_file:"SHA256":"data_files/hash_file_4":"e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855"

generic SHA-384 Hash file #1
depends_on:MBEDTLS_SHA512_C
mbedtls_md_file:"SHA384":"data_files/hash_file_1":"e0a3e6259d6378001b54ef82f5dd087009c5fad86d8db226a9fe1d14ecbe33a6fc916e3a4b16f5f286424de15d5a8e0e"

generic
SHA-384 Hash file #2
depends_on:MBEDTLS_SHA512_C
mbedtls_md_file:"SHA384":"data_files/hash_file_2":"eff727afc8495c92e2f370f97a317f93c3350324b0646b0f0e264708b3c97d3d332d3c5390e1e47130f5c92f1ef4b9cf"

generic SHA-384 Hash file #3
depends_on:MBEDTLS_SHA512_C
mbedtls_md_file:"SHA384":"data_files/hash_file_3":"6fc10ebda96a1ccf61777cac72f6034f92533d42052a4bf9f9d929c672973c71e5aeb1213268043c21527ac0f7f349c4"

generic SHA-384 Hash file #4
depends_on:MBEDTLS_SHA512_C
mbedtls_md_file:"SHA384":"data_files/hash_file_4":"38b060a751ac96384cd9327eb1b1e36a21fdb71114be07434c0cc7bf63f6e1da274edebfe76f65fbd51ad2f14898b95b"

generic SHA-512 Hash file #1
depends_on:MBEDTLS_SHA512_C
mbedtls_md_file:"SHA512":"data_files/hash_file_1":"d8207a2e1ff2b424f2c4163fe1b723c9bd42e464061eb411e8df730bcd24a7ab3956a6f3ff044a52eb2d262f9e4ca6b524092b544ab78f14d6f9c4cc8ddf335a"

generic SHA-512 Hash file #2

depends_on:MBEDTLS_SHA512_C
mbedtls_md_file:"SHA512":"data_files/hash_file_2":"ecbb7f0ed8a702b49f16ad3088bcc06ea93451912a7187db15f
64d93517b09630b039293aed418d4a00695777b758b1f381548c2fd7b92ce5ed996b32c8734e7"

generic
SHA-512 Hash file #3
depends_on:MBEDTLS_SHA512_C
mbedtls_md_file:"SHA512":"data_files/hash_file_3":"7ccc9b2da71ffde9966c3ce44d7f20945fccf33b1fade4da152b0
21f1afcc7293382944aa6c09eac67af25f22026758e2bf6bed86ae2a43592677ee50f8eea41"

generic SHA-512 Hash file #4
depends_on:MBEDTLS_SHA512_C
mbedtls_md_file:"SHA512":"data_files/hash_file_4":"cf83e1357eefb8bdf1542850d66d8007d620e4050b5715dc83f
4a921d36ce9ce47d0d13c5d85f2b0ff8318d2877eec2f63b931bd47417a81a538327af927da3e"
-----BEGIN CERTIFICATE-----
MIIB/TCCAYCgAwIBAgIBATAMBggqhkjOPQQDAgUAMD4xCzAJBgNVBAYTAk5MMREw
DwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBFQyBDQTAe
Fw0wMzA5MjQxNTQ5NDhaFw0xMzA5MjQxNTQ5NDhaMD4xCzAJBgNVBAYTAk5MMREw
DwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBFQyBDQTB2
MBAGByqGSM49AgEGBSuBBAAiA2IABMPaKzRBN1gvh1b+/Im6KUNLTuBuww5XUzM5
WNRStJGVOQsj318XJGJI/BqVKc4sLYfCiFKAr9ZqqyHduNMcbli4yuiyaY7zQa0p
w7RfdadHb9UZKVVpmlM7ILRmFmAzHqNQME4wDAYDVR0TBAUwAwEB/zAdBgNVHQ4E
FgQUnW0gJEkBPyvLeLUZvH4kydv7NnwwHwYDVR0jBBgwFoAUnW0gJEkBPyvLeLUZ
vH4kydv7NnwwDAYIKoZIzj0EAwIFAANpADBmAjEAvQ/49lXXrLYdOIGtTaYWjpZP
tRBXQiGPMzUvmKBk7gM7bF4iFPsdJikyXHmuwv3RAjEA8vtUX8fAAB3fbh5dEXRm
l7tz0Sw/RW6AHFtaIauGkhHqeKIaKIi6WSgHu6x97uyg
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIICUjCCAdegAwIBAgIJAMFD4n5iQ8zoMAoGCCqGSM49BAMCMD4xCzAJBgNVBAYT
Ak5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBF
QyBDQTAeFw0xMzA5MjQxNTQ5NDhaFw0yMzA5MjIxNTQ5NDhaMD4xCzAJBgNVBAYT
Ak5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBF
QyBDQTB2MBAGByqGSM49AgEGBSuBBAAiA2IABMPaKzRBN1gvh1b+/Im6KUNLTuBu
ww5XUzM5WNRStJGVOQsj318XJGJI/BqVKc4sLYfCiFKAr9ZqqyHduNMcbli4yuiy
aY7zQa0pw7RfdadHb9UZKVVpmlM7ILRmFmAzHqOBoDCBnTAdBgNVHQ4EFgQUnW0g
JEkBPyvLeLUZvH4kydv7NnwwbgYDVR0jBGcwZYAUnW0gJEkBPyvLeLUZvH4kydv7
NnyhQqRAMD4xCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UE
AxMTUG9sYXJzc2wgVGVzdCBFQyBDQYIJAMFD4n5iQ8zoMAwGA1UdEwQFMAMBAf8w
CgYIKoZIzj0EAwIDaQAwZgIxAMO0YnNWKJUAfXgSJtJxexn4ipg+kv4znuR50v56
t4d0PCu412mUC6Nnd7izvtE2MgIxAP1nnJQjZ8BWukszFQDG48wxCCyci9qpdSMv
uCjn8pwUOkABXK8Mss90fzCfCEOtIA==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDhTCCAm2gAwIBAgIBBDANBgkqhkiG9w0BAQsFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UECgwIUG9sYXJTU0wxGTAXBgNVBAMMEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTcwNTA1MTMwNzU5WhcNMjcwNTA2MTMwNzU5WjA8MQswCQYDVQQGEwJOTDERMA8G
A1UECgwIUG9sYXJTU0wxGjAYBgNVBAMMEVBvbGFyU1NMIENsaWVudCAyMIIBIjAN

BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAyHTEzLn5tXnpRdkUYLB9u5Pyax6f
M60Nj4o8VmXl3ETZzGaFB9X4J7BKNdBjngpuG7fa8H6r7gwQk4ZJGDTzqCrSV/Uu
1C93KYRhTYJQj6eVSHD1bk2y1RPD0hrt5kPqQhTrdOrA7R/UV06p86jt0uDBMHEw
MjDV0/YI0FZPRo7yX/k9Z5GIMC5Cst99++UMd//sMcB4j7/Cf8qtbCHWjdmLao5v
4Jv4EFbMs44TFeY0BGbH7vk2DmqV9gmaBmf0ZXH4yqSxJeD+PIs1BGe64E92hfx/
/DZrtenNLQNiTrM9AM+vdqBpVoNq0qjU51Bx5rU2BXcFbXvI5MT9TNUhXwIDAQAB
o4GSMIGPMB0GA1UdDgQWBBRxoQBzckAvVHZeM/xSj7zx3WtGITBjBgNVHSMEXDBa
gBS0WuSls97SUva51aaVD+s+vMf9/6E/pD0wOzELMAkGA1UEBhMCTkwxETAPBgNV
BAoMCFBvbGFyU1NMMRkwFwYDVQQDDBBQb2xhclNTTCBUZXN0IENBggEAMAkGA1Ud
EwQCMAAwDQYJKoZIhvcNAQELBQADggEBAC7yO786NvcHpK8UovKIG9cB32oSQQom
LoR0eHDRzdqEkoq7yGZufHFiRAAzbMqJfogRtxlrWAeB4y/jGaMBV25IbFOIcH2W
iCEaMMbG+VQLKNvuC63kmw/Zewc9ThM6Pa1Hcy0axT0faf1B/U01j0FIcw/6mTfK
D8w48OIwc1yr0JtutCVjig5DC0yznGMt32RyseOLcUe+lfq005v2PAiCozr5X8rE
ofGZpiM2NqRPePgYy+Vc75Zk28xkRQq1ncprgQb3S4vTsZdScpM9hLf+eMlrgqlj
c5PLSkXBeLE5+fedkyfTaLxxQlgCpuoOhKBm04/R1pWNzUHyqagjO9Q=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIC9DCCAdygAwIBAAIBATANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTEwMjEyMTQ0NDA2WhcNMjEwMjEyMTQ0NDA2WjA8MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxGjAYBgNVBAMTEVBvbGFyU1NMIFNlcnZlciAxMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqQIfPUBq1VVTi/027oJlLhVhXom/
uOhFkNvuiBZS0/FDUEeWEllkh2v9K+BG+XO+3c+S4ZFb7Wagb4kpeUWA0INq1UFD
d185fAkER4KwVzlw7aPsFRkeqDMIR8EFQqn9TMO0390GH00QUUBncxMPQPhtgSVf
CrFTxjB+FTms+Vruf5KepgVb5xOXhbUjktnUJAbVCSWJdQfdphqPPwkZvq1lLGTr
lZvc/kFeF6babFtpzAK6FCwWJJxK3M3Q91Jnc/EtoCP9fvQxyi1wyokLBNsupk9w
bp7OvViJ4lNZnm5akmXiiD8MlBmj3eXonZUT7Snbq3AS3FrKaxerUoJUsQIDAQAB
owIwADANBgkqhkiG9w0BAQUFAAOCAQEAoZVuVi7bIslKgMJhejSFXiO+ICMz1fmK
b0tPN68mRYhI/gsjRT0cmX6GUNrg+U5mcBWhMwHgyvx1CARU4YToKZxcXGNL0DPd
Z1hF8nCrJCZBQvNuWE7s0ufw92xz5ZfuKkVxi94RYR529F6gzgl4rpX8UQVu2ym/
9pTlHKr4MKi9LNppyJMS89uRcb2FJFMdhAKbhNtbIjI9qGZ7x//0belAaWhq389u
6XWFnZt35PU6Zz6YbAQ5pjZYsTaohuufgrpOlFPUuc4uR+RfGHIQ6id12lZaQC2m
OFIBDcU0x1cFfPfMgVdBLf6klPt/v/tD77mwx0eztSp28NIf+ACw8A==
-----END
CERTIFICATE-----
-----BEGIN EC PARAMETERS-----
BggqhkjOPQMBBw==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIKEycJNLyYJ5JgECpCuZiFeXZIMC+XsMEKoMhRTx6xD+oAoGCCqGSM49
AwEHoUQDQgAE0TGTdER8z3aJzZmbqvVz4c70Odk2qJMU9/aqULZRcr1LhBiqy6Db
3XKQEWgNKxqbrekSwEDlVIjVZSdyKY+/PQ==
-----END EC PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIC+jCCAeKgAwIBAgIBATANBgkqhkiG9w0BAQsFADAWMRQwEgYDVQQDEwtUZXN0
IHJvb3QgMjAeFw0wMTAxMDEwMDAwMDBaFw0zMDEyMzEyMzU5NTlaMBYxFDASBgNV
BAMTC1Rlc3Qgcm9vdCAyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA

mTX2sHY42Ord9gWyB6GcdlLjjE+4zBJ1BoDpMnvJ89niMTuZTq1ViMp/B6RuTH+2
YF3+riZYQDH9yM/8rgvAUIvK9STaq19Zrm0mnfQUo9yKdkfoJ+XvWuvK6f+NkAMg
xfhAD6eSupigTvov/w2IT8rS0dxo4KF6hKBL2aYlXhiEyi/NmsEPZWvVh+qk3L/Q
GSwpgC+DhVoQzFRofUdK9O9MkgR675iftaFDvyi7F0fxrSLfB/Wy4cgRYzIW6pyN
2sXWivKdLI3bgB01ffdbO17ZAGILK1whO29/bX6hbH09Y/H7jR2vjy+KP9N0PEa3
7SBymlokB3A8wq/LWPYPeQIDAQABo1MwUTAPBgNVHRMECDAGAQEBAgEBMB0GA1Ud
DgQWBBSOBd1fH00Y9r5S8cELj/9IT4BGlDAfBgNVHSMEGDAWgBSOBd1fH00Y9r5S
8cELj/9IT4BGlDANBgkqhkiG9w0BAQsFAAOCAQEAB9nLaqxsBW0isDaBGNJyzH9O
WqYY0hex9tm3UqygfE9b9aahykpkowQIzh4D9Xpbd0hZGVlK/sw2qsKj6gDOiMtL
uWs4gaFNWIQqhVsTzL88c7XaW55n+TRQdVZyy38DZVWphte1Mumc9WB8N15rZTDh
iXjwGl0mrV1egq4hJZLpy14f6ihqU7KGfmc9onxvgvWxYLi+5v8874c4ophSKsI2
qVE8iZ6uq2oQ66Pd5S50cYk6MEW5lifAhLM5WFZmW7dRKmykBGZ9rFrJrIvhkmh9
He7q6TEQP1Wcoc147nIg0BTkHGtdrEv3jIX6UKKUEwUUk9ARB1mSodZQHBhuww==
-----END
CERTIFICATE-----
00 0
*H=0>10 UNL10U
PolarSSL10UPolarssl Test EC CA0
130924155204Z
230922155204Z0410 UNL10U
PolarSSL10U localhost0Y0*H=*H=B7Vv Zr>Y- n|th"YbN#/4]]kw
U*00 U00UPaecF0nU#g0em $I?+x~$6|B@0>10 UNL10U
PolarSSL10UPolarssl Test EC CA C~bC0
*H=h0e1,\d
Na1ssT]/!)5>90!6]'%;5%Y^|f{Os!R*_
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 17 (0x11)
  Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=NL, O=PolarSSL, CN=PolarSSL Test CA
    Validity
      Not Before: May 10 13:23:41 2012 GMT
      Not After : May 11 13:23:41 2022 GMT
    Subject: C=NL, O=PolarSSL, CN=www.example.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
        Modulus:
          00:b9:3c:4a:c5:c8:a3:8e:90:17:a4:9e:52:aa:71:
          75:26:61:80:e7:c7:b5:6d:8c:ff:aa:b6:41:26:b7:
          be:11:ad:5c:73:16:0c:64:11:48:04:ff:d6:e1:3b:
          05:db:89:bb:b3:97:09:d5:1c:14:dd:68:87:39:b0:
          3d:71:cb:e2:76:d0:1a:d8:18:2d:80:1b:54:f6:e5:
          44:9a:f1:cb:af:61:2e:df:49:0d:9d:09:b7:ed:b1:
          fd:3c:fd:3c:fa:24:cf:5d:bf:7c:e4:53:e7:25:b5:
          ea:44:22:e9:26:d3:ea:20:94:9e:e6:61:67:ba:2e:

```
            07:67:0b:03:2f:a2:09:ed:f0:33:8f:0b:ce:10:ef:
            67:a4:c6:08:da:c1:ed:c2:3f:d7:4a:dd:15:3d:f9:
            5e:1c:81:60:46:3e:b5:b3:3d:2f:a6:de:47:1c:bc:
            92:ae:eb:df:27:6b:16:56:b7:dc:ec:d1:55:57:a5:
            6e:ec:75:25:f5:b7:7b:df:ab:d2:3a:5a:91:98:7d:
            97:17:0b:13:0a:a7:6b:4a:8b:c1:47:30:fb:3a:f8:
            41:04:d5:c1:df:b8:1d:bf:7b:01:a5:65:a2:e0:1e:
            36:b7:a6:5c:cc:30:5a:f8:cd:6f:cd:f1:19:62:25:
            ca:01:e3:35:7f:fa:20:f5:dc:fd:69:b2:6a:00:7d:
            17:f7
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints:
        CA:FALSE
      X509v3 Subject Key Identifier:
        7D:E4:9C:6B:E6:F9:71:7D:46:D2:12:3D:AD:6B:1D:FD:C2:AA:78:4C
      X509v3 Authority Key Identifier:
        keyid:B4:5A:E4:A5:B3:DE:D2:52:F6:B9:D5:A6:95:0F:EB:3E:BC:C7:FD:FF

      X509v3 Subject Alternative Name:
        DNS:example.com, DNS:example.net, DNS:*.example.org
  Signature Algorithm: sha1WithRSAEncryption
    4f:09:cb:7a:d5:ee:f5:ef:62:0d:dc:7b:a2:85:d6:8c:ca:95:
    b4:6b:da:11:5b:92:00:75:13:b9:ca:0b:ce:ea:fb:c3:1f:e2:
    3f:7f:21:74:79:e2:e6:bc:da:06:e5:2f:6f:f6:55:c6:73:39:
    cf:48:bc:0d:2f:0c:d2:7a:06:c3:4a:4c:d9:48:5d:a0:d0:73:
    89:e4:d4:85:1d:96:9a:0e:57:99:c6:6f:1d:21:27:1f:8d:05:
    29:e8:40:ae:82:39:68:c3:97:07:cf:3c:93:4c:1a:df:2f:a6:
    a4:55:48:7f:7c:8c:1a:c9:22:da:24:cd:92:39:c6:8a:ec:b0:
    8d:f5:69:82:67:cb:04:ee:de:53:41:96:c1:27:dc:2f:fe:33:
    fa:d3:0e:b8:d4:32:a9:84:28:53:a5:f0:d1:89:d5:a2:98:e7:
    16:91:bb:9c:c0:41:8e:8c:58:ac:ff:e3:dd:2e:7a:ab:b0:b9:
    71:76:ad:0f:27:33:f7:a9:29:d3:c0:76:c0:bf:06:40:7c:0e:
    d5:a4:7c:8a:e2:32:6e:16:ae:da:64:1f:b0:55:7c:db:dd:f1:
    a4:ba:44:7c:b3:99:58:d2:34:6e:00:ea:97:6c:14:3a:f2:10:
     1e:0a:a2:49:10:76:01:f4:f2:c8:18:fd:cc:63:46:12:8b:09:
    1b:f1:94:e6
-----BEGIN CERTIFICATE-----
MIIDcjCCAlqgAwIBAgIBETANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTIwNTEwMTMyMzQxWhcNMjIwNTExMTMyMzQxWjA6MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxGDAWBgNVBAMTD3d3dy5leGFtcGxlLmNvbTCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBALk8SsXIo46QF6SeUqpxdSZhgOfHtW2M
/6q2QSa3vhGtXHMWDGQRSAT/1uE7BduJu7OXCdUcFN1ohzmwPXHL4nbQGtgYLYAb
VPblRJrxy69hLt9JDZ0Jt+2x/Tz9PPokz12/fORT5yW16kQi6SbT6iCUnuZhZ7ou
B2cLAy+iCe3wM48LzhDvZ6TGCNrB7cI/10rdFT35XhyBYEY+tbM9L6beRxy8kq7r
3ydrFla33OzRVVelbux1JfW3e9+r0jpakZh9lxcLEwqna0qLwUcw+zr4QQTVwd+4
Hb97AaVlouAeNremXMwwWvjNb83xGWIlygHjNX/6IPXc/WmyagB9F/cCAwEAAaOB
```

```
gTB/MAkGA1UdEwQCMAAwHQYDVR0OBBYEFH3knGvm+XF9RtISPa1rHf3CqnhMMB8G
A1UdIwQYMBaAFLRa5KWz3tJS9rnVppUP6z68x/3/MDIGA1UdEQQrMCmCC2V4YW1w
bGUuY29tggtleGFtcGxlLm5ldIINKi5leGFtcGxlLm9yZzANBgkqhkiG9w0BAQUF
AAOCAQEATwnLetXu9e9iDdx7ooXWjMqVtGvaEVuSAHUTucoLzur7wx/iP38hdHni
5rzaBuUvb/ZVxnM5z0i8DS8M0noGw0pM2UhdoNBzieTUhR2Wmg5XmcZvHSEnH40F
KehAroI5aMOXB888k0wa3y+mpFVIf3yMGski2iTNkjnGiuywjfVpgmfLBO7eU0GW
wSfcL/4z+tMOuNQyqYQoU6Xw0YnVopjnFpG7nMBBjoxYrP/j3S56q7C5cXatDycz
96kp08B2wL8GQHwO1aR8iuIybhau2mQfsFV8293xpLpEfLOZWNI0bgDql2wUOvIQ
HgqiSRB2AfTyyBj9zGNGEosJG/GU5g==
-----END
 CERTIFICATE-----
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
   <Configuration>Release</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\hash\hello.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">
   <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
   </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid>{B02D4AE1-0218-1CD4-F44E-EFAE19B01B8D}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>hello</RootNamespace>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
```

```
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
/>
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <LinkIncremental>true</LinkIncremental>
```

```
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
     <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
 <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
```

```
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
   </Link>
   <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
   </ProjectReference>
  </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
   <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
   </Link>
  </ItemDefinitionGroup>
   <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
   <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
   <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
   </Link>
  </ItemDefinitionGroup>
```

<Import Project="$(VCTargetsPath)\Microsoft.Cpp.targets"
/>
<ImportGroup Label="ExtensionTargets">
</ImportGroup>
</Project>
RSA PKCS1 Verify v1.5 CAVS #1
depends_on:MBEDTLS_SHA1_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"d6248c3e96b1a7e5fea978870fcc4c9786b4e5156e16b7faef4557d667f730b8bc4c784ef0
0c624df5309513c3a5de8ca94c2152e0459618666d3148092562ebc256ffca45b27fd2d63c68bd5e0a0aefbe496e9e638
38a361b1db6fc272464f191490bf9c029643c49d2d9cd08833b8a70b4b3431f56fb1eb55ccd39e77a9c92":MBEDTLS
_RSA_PKCS_V15:MBEDTLS_MD_SHA1:1024:16:"e28a13548525e5f36dccb24ecb7cc332cc689dfd64012604c9c
7816d72a16c3f5fcdc0e86e7c03280b1c69b586ce0cd8aec722cc73a5d3b730310bf7dfebdc77ce5d94bbc369dc18a2f7
b07bd505ab0f82224aef09fdc1e5063234255e0b3c40a52e9e8ae60898eb88a766bdd788fe9493d8fd86bcdd2884d5c06
216c65469e5":16:"3":"3203b7647fb7e345aa457681e5131777f1adc371f2fba8534928c4e52ef6206a856425d626935
2ecbf64db2f6ad82397768cafdd8cd272e512d617ad67992226da6bc291c31404c17fd4b7e2beb20eff284a44f4d7af47f
d6629e2c95809fa7f2241a04f70ac70d3271bb13258af1ed5c5988c95df7fa26603515791075feccd":MBEDTLS_ERR
_RSA_VERIFY_FAILED

RSA PKCS1 Verify v1.5 CAVS #2
depends_on:MBEDTLS_SHA1_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"206ef4bf396c6087f8229ef196fd35f37ccb8de5efcdb238f20d556668f114257a11fbe0384
64a67830378e62ae9791453953dac1dbd7921837ba98e84e856eb80ed9487e656d0b20c28c8ba5e35db1abbed83ed1c
7720a97701f709e3547a4bfcabca9c89c57ad15c3996577a0ae36d7c7b699035242f37954646c1cd5c08ac":MBEDTLS
_RSA_PKCS_V15:MBEDTLS_MD_SHA1:1024:16:"e28a13548525e5f36dccb24ecb7cc332cc689dfd64012604c9c
7816d72a16c3f5fcdc0e86e7c03280b1c69b586ce0cd8aec722cc73a5d3b730310bf7dfebdc77ce5d94bbc369dc18a2f7
b07bd505ab0f82224aef09fdc1e5063234255e0b3c40a52e9e8ae60898eb88a766bdd788fe9493d8fd86bcdd2884d5c06
216c65469e5":16:"3":"5abc01f5de25b70867ff0c24e222c61f53c88daf42586fddcd56f3c4588f074be3c328056c06338
8688b6385a8167957c6e5355a510e005b8a851d69c96b36ec6036644078210e5d7d326f96365ee0648882921492bc7b
753eb9c26cdbab37555f210df2ca6fec1b25b463d38b81c0dcea202022b04af5da58aa03d77be949b7":0

RSA
PKCS1 Verify v1.5 CAVS #3
depends_on:MBEDTLS_SHA1_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"206ef4bf396c6087f8229ef196fd35f37ccb8de5efcdb238f20d556668f114257a11fbe0384
64a67830378e62ae9791453953dac1dbd7921837ba98e84e856eb80ed9487e656d0b20c28c8ba5e35db1abbed83ed1c
7720a97701f709e3547a4bfcabca9c89c57ad15c3996577a0ae36d7c7b699035242f37954646c1cd5c08ac":MBEDTLS
_RSA_PKCS_V15:MBEDTLS_MD_SHA1:1024:16:"e28a13548525e5f36dccb24ecb7cc332cc689dfd64012604c9c
7816d72a16c3f5fcdc0e86e7c03280b1c69b586ce0cd8aec722cc73a5d3b730310bf7dfebdc77ce5d94bbc369dc18a2f7
b07bd505ab0f82224aef09fdc1e5063234255e0b3c40a52e9e8ae60898eb88a766bdd788fe9493d8fd86bcdd2884d5c06
216c65469e5":16:"3":"5abc01f5de25b70867ff0c24e222c61f53c88daf42586fddcd56f3c4588f074be3c328056c06338
8688b6385a8167957c6e5355a510e005b8a851d69c96b36ec6036644078210e5d7d326f96365ee0648882921492bc7b
753eb9c26cdbab37555f210df2ca6fec1b25b463d38b81c0dcea202022b04af5da58aa03d77be949b7":0

RSA
PKCS1 Verify v1.5 CAVS #4
depends_on:MBEDTLS_SHA256_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"867ac26e11a13b7ac34a42a1e177648692861226effb55bb597fbde10f299bf7fffd6fc8ddb
2a46a73b97b67387a461b23e1d65dc119366286979add615b926b9272832fc0c058b946fc752dcffceca12233f4c63f78

97cbaa08aa7e07cf02b5e7e3e5ece252bf2fe61d163bce84c0e0368454a98e9fdebf6edbd70b290d549b":MBEDTLS_RSA_PKCS_V15:MBEDTLS_MD_SHA224:1024:16:"e28a13548525e5f36dccb24ecb7cc332cc689dfd64012604c9c7816d72a16c3f5fcdc0e86e7c03280b1c69b586ce0cd8aec722cc73a5d3b730310bf7dfebdc77ce5d94bbc369dc18a2f7b07bd505ab0f82224aef09fdc1e5063234255e0b3c40a52e9e8ae60898eb88a766bdd788fe9493d8fd86bcdd2884d5c06216c65469e5":16:"3":"3bb7b1c5f3391de4549e2e96fd33afa4d647dd90e321d9d576f3808e32213e948b697ef4fd2dd12923de6ec3ffd625078a57f86af38dc07052bb50547c616ed51fa1352b3ab66788408168d21263ef2d3388d567d2ce8cf674f45491ab2b0319d47be1266bda39e343b2a38ea2d6aaaee6c4465aee1d7bb33e93a1c40a8e3ae4":0

RSA
PKCS1 Verify v1.5 CAVS #5
depends_on:MBEDTLS_SHA256_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"cd810e97dc21095ea7a0238027a7bafd343e01444785ea9184a44a79f80438c41fc0b57aa95693407da38fe5ff0ec1398e03361e51a3dbe134b99cca2df0cef1c444ca54d2b7db2789455b6bb41918c24001fd82fc20ee089de3f34f053699c1c5f7954ce0aaabb9d26fce39d032894152229d98cf64ecafc7089530073c61d9":MBEDTLS_RSA_PKCS_V15:MBEDTLS_MD_SHA256:1024:16:"e28a13548525e5f36dccb24ecb7cc332cc689dfd64012604c9c7816d72a16c3f5fcdc0e86e7c03280b1c69b586ce0cd8aec722cc73a5d3b730310bf7dfebdc77ce5d94bbc369dc18a2f7b07bd505ab0f82224aef09fdc1e5063234255e0b3c40a52e9e8ae60898eb88a766bdd788fe9493d8fd86bcdd2884d5c06216c65469e5":16:"3":"7b5fba70ec5b521638f182bcab39cec30b76e7bc017bdbd1059658a9a1db0969ab482dce32f3e9865952f0a0de0978272c951e3c015328ea3758f47029a379ab4200550fba58f11d51264878406fc717d5f7b72b3582946f16a7e5314a220881fc820f7d29949710273421533d8ac0a449dc6d0fd1a21c22444edd1c0d5b44d3":0

RSA
PKCS1 Verify v1.5 CAVS #6
depends_on:MBEDTLS_SHA512_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"44637d3b8de525fd589237bc81229c8966d3af24540850c24036330db8007e6d19a19486018b2b02074da590aaba9d2c8848c0a2d1b6de4dfaf24025b6393df9228008f83f13cc76a67cfbed77a6e3429342824a0b6a9b8dd884094acc6a54bbc8c8829930c52fe39ce5e0dcd02d9553ef899d26eb6cae0940b63584e2daeb3b":MBEDTLS_RSA_PKCS_V15:MBEDTLS_MD_SHA384:1024:16:"e28a13548525e5f36dccb24ecb7cc332cc689dfd64012604c9c7816d72a16c3f5fcdc0e86e7c03280b1c69b586ce0cd8aec722cc73a5d3b730310bf7dfebdc77ce5d94bbc369dc18a2f7b07bd505ab0f82224aef09fdc1e5063234255e0b3c40a52e9e8ae60898eb88a766bdd788fe9493d8fd86bcdd2884d5c06216c65469e5":16:"3":"38fc4f6f0430bb3ea9f470a4c0f5cebdabac4dbeb3b9c99d4168e7b00f5eb294ec0ece1908ded1f3e14f1e69d10f9feb425bda0c998af945ef864298a60a675f0bb5c540a7be3f534d5faddff974eea8bffe182a44e2ee1f4f653e71967a11869ee1a850edb03cb44a340378cb7a1bc9616d3649b78002b390a05a7e54edec6":0

RSA
PKCS1 Verify v1.5 CAVS #7
depends_on:MBEDTLS_SHA512_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"d03f12276f6ba7545b8fce719471bd253791878809694e8754f3b389f26c9253a758ed28b4c62535a8d5702d7a778731d5759ff2b3b39b192db680e791632918b6093c0e8ca25c2bf756a07fde4144a37f769fe4054455a45cb8cefe4462e7a9a45ce71f2189b4fef01b47aee8585d44dc9d6fa627a3e5f08801871731f234cd":MBEDTLS_RSA_PKCS_V15:MBEDTLS_MD_SHA384:1024:16:"e28a13548525e5f36dccb24ecb7cc332cc689dfd64012604c9c7816d72a16c3f5fcdc0e86e7c03280b1c69b586ce0cd8aec722cc73a5d3b730310bf7dfebdc77ce5d94bbc369dc18a2f7b07bd505ab0f82224aef09fdc1e5063234255e0b3c40a52e9e8ae60898eb88a766bdd788fe9493d8fd86bcdd2884d5c06216c65469e5":16:"3":"d93a878c1ce86571590b0e43794b3edb23552797c4b8c9e3da4fe1cc4ac0566acd3b10541fe9a7a79f5ea4892d3069ca6903efb5c40c47eb8a9c781eb4249281d40c3d96aae16da1bb4daaece6a26eca5f41c062b4124a64fc9d340cba5ab0d1f5affff6515a87f0933774fd4322d2fa497cd6f708a429ca56dcb1fd3db623d0":MBEDTLS_ERR_RSA_INVALID_PADDING

RSA
PKCS1 Verify v1.5 CAVS #8
depends_on:MBEDTLS_SHA512_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"b2f2e6e09fd19b0a8c06447554d6a236c69e2b334017488881d8c02ab81d74cae0c64efd5
0a374998eeec162651975e637cb2ba594250c750a4943253f1db0613e4ce1d50f8e3e968a2a83bd6cb97455ab2ccc770
71076b3e211ffb251bd4c1a738b88b2021c61c727c074ce933c054acbcbf4f0c362ec09af38de191686aebe":MBEDTL
S_RSA_PKCS_V15:MBEDTLS_MD_SHA512:1024:16:"e28a13548525e5f36dccb24ecb7cc332cc689dfd64012604
c9c7816d72a16c3f5fcdc0e86e7c03280b1c69b586ce0cd8aec722cc73a5d3b730310bf7dfebdc77ce5d94bbc369dc18a
2f7b07bd505ab0f82224aef09fdc1e5063234255e0b3c40a52e9e8ae60898eb88a766bdd788fe9493d8fd86bcdd2884d5
c06216c65469e5":16:"3":"a853e67f928281d11506c9d39e5ea9b2d742782c663c37d0a7c9e9fe15379cde1e75d94adb
fb1ca08691f320af4ff2b0a29a4d2ea10a20cb95d85f3dabac3d56cca9039c851d0181408c00b385fc82cafa4cfa7380d0c
2c024fb83fec59d5ee591d63806dcb18b21ea440c3d3f12c1e7795eb15b7ce4c4b288d646cf1d34bdf1":0

RSA
PKCS1 Verify v1.5 CAVS #9
depends_on:MBEDTLS_SHA1_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"647586ba587b09aa555d1b8da4cdf5c6e777e08859379ca45789019f2041e708d97c4408d
4d6943b11dd7ebe05c6b48a9b5f1b0079452cc484579acfa66a34c0cf3f0e7339b2dbd5f1339ef7937a8261547705a846
885c43d8ef139a9c83f5604ea52b231176a821fb48c45ed45226f31ba7e8a94a69f6c65c39b7278bf3f08f":MBEDTLS_
RSA_PKCS_V15:MBEDTLS_MD_SHA1:1024:16:"e28a13548525e5f36dccb24ecb7cc332cc689dfd64012604c9c7
816d72a16c3f5fcdc0e86e7c03280b1c69b586ce0cd8aec722cc73a5d3b730310bf7dfebdc77ce5d94bbc369dc18a2f7b
07bd505ab0f82224aef09fdc1e5063234255e0b3c40a52e9e8ae60898eb88a766bdd788fe9493d8fd86bcdd2884d5c062
16c65469e5":16:"10001":"e27a90b644c3a11f234132d6727ada397774cd7fdf5eb0160a665ffccedabb8ae9e35796693
9a71c973e75e5ff771fb01a6483fcaf82f16dee65e6826121e2ae9c69d2c92387b33a641f397676776cde501e7314a9a4e
76c0f4538edeea163e8de7bd21c93c298df748c6f5c26b7d03bfa3671f2a7488fe311309e8218a71171":0

RSA
PKCS1 Verify v1.5 CAVS #10
depends_on:MBEDTLS_SHA1_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"55013a489e09b6553262aab59fb041b49437b86d52876f8e5d5e405b77ca0ff6ce8ea2dd7
5c7b3b411cf4445d56233c5b0ff0e58c49128d81b4fedd295e172d225c451e13defb34b87b7aea6d6f0d20f5c55feb71d
2a789fa31f3d9ff47896adc16bec5ce0c9dda3fde190e08ca2451c01ff3091449887695f96dac97ad6a30e":MBEDTLS_
RSA_PKCS_V15:MBEDTLS_MD_SHA1:1024:16:"e28a13548525e5f36dccb24ecb7cc332cc689dfd64012604c9c7
816d72a16c3f5fcdc0e86e7c03280b1c69b586ce0cd8aec722cc73a5d3b730310bf7dfebdc77ce5d94bbc369dc18a2f7b
07bd505ab0f82224aef09fdc1e5063234255e0b3c40a52e9e8ae60898eb88a766bdd788fe9493d8fd86bcdd2884d5c062
16c65469e5":16:"10001":"dd82b7be791c454fbbf6f1de47cbe585a687e4e8bbae0b6e2a77f8ca4efd06d71498f9a74b9
31bd59c377e71daf708a624c51303f377006c676487bad57f7067b09b7bb94a6189119ab8cf7321c321b2dc7df565bfbe
c833a28b86625fb5fd6a035d4ed79ff0f9aee9fa78935eec65069439ee449d7f5249cdae6fdd6d8c2a63":MBEDTLS_ER
R_RSA_INVALID_PADDING

RSA
PKCS1 Verify v1.5 CAVS #11
depends_on:MBEDTLS_SHA256_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"f4a990b8d434a5914340c0ca3ca4e4a70856c55e13e938c1f854e91cdef54c6107d6d682a6
2e6c1ff12b1c6178ee0b26b5d8ae5ee4043db4151465727f313e9e174d7c6961abe9cb86a21367a89e41b47267ac5ef3a
6eceaaca5b19ae756b3904b97ec35aeb404dc2a2d0da373ba709a678d2728e7d72daae68d335cbf6c957d":MBEDTLS
_RSA_PKCS_V15:MBEDTLS_MD_SHA224:1024:16:"e28a13548525e5f36dccb24ecb7cc332cc689dfd64012604c
9c7816d72a16c3f5fcdc0e86e7c03280b1c69b586ce0cd8aec722cc73a5d3b730310bf7dfebdc77ce5d94bbc369dc18a2f

7b07bd505ab0f82224aef09fdc1e5063234255e0b3c40a52e9e8ae60898eb88a766bdd788fe9493d8fd86bcdd2884d5c0
6216c65469e5":16:"10001":"d8ef7bdc0f111b1249d5ad6515b6fe37f2ff327f493832f1385c10e975c07b0266497716f
cb84f5039cd60f5a050614fde27f354a6c45e8a7d74f9821e2f301500ac1953feafeb9d98cf88d2c928413f337813135c6
6abfc3dc7a4d80655d925bf96f21872ca2b3a2684b976ca768fe37feae20a69eeec3cc8f1de0db34b3462":0

RSA
PKCS1 Verify v1.5 CAVS #12
depends_on:MBEDTLS_SHA256_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"c81f04c79982971fa176d64e8f7f8812f86a94c49e84672ff10996a2d6dfc444a884c7a87c4
606a1aab22558894ee59b798b457827f5ee0b0cadcd94371902cc4ddaf97acefed641997717bcb3cc74cd440f0a31e20f
b95812cecb740c36d6d1bf07e3641514cfa678aff2a39562ff4d60e02b17583a92bf0c56d66bde9e09f8":MBEDTLS_R
SA_PKCS_V15:MBEDTLS_MD_SHA256:1024:16:"e28a13548525e5f36dccb24ecb7cc332cc689dfd64012604c9c7
816d72a16c3f5fcdc0e86e7c03280b1c69b586ce0cd8aec722cc73a5d3b730310bf7dfebdc77ce5d94bbc369dc18a2f7b
07bd505ab0f82224aef09fdc1e5063234255e0b3c40a52e9e8ae60898eb88a766bdd788fe9493d8fd86bcdd2884d5c062
16c65469e5":16:"10001":"52111f4798da3c11b3c74394358348ab0fc797bde99080f238d33a69b04b08ac2bd767b33
872473943e23af27ca32fd568a43a8c7d6cc55b4fbb380212fdfcb60487e20694d4287e233efdf7b04737c0037a592d03
077801828b051998c42b9f9e2420063331d5b2349918a64d8b65b21a2011ee7318fcef48aced95b8ddf501":0

RSA
PKCS1 Verify v1.5 CAVS #13
depends_on:MBEDTLS_SHA512_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"a97824871770b79da979a111f6decfb1dd11bd946cfa800b008f0ad5aea5aa92e205d27a46
c31d4fe6cb909091bd21f082fb75074000ee46c2f3e530d77b34c7c5d6f8453025950d3e0afae1f9752655f5bbea8432e9
f1014357ff11b08076179a101e4f9d3f25bffb5e656bf6afe6c97d7aa4740b5d9224cde4dede035a7768":MBEDTLS_R
SA_PKCS_V15:MBEDTLS_MD_SHA384:1024:16:"e28a13548525e5f36dccb24ecb7cc332cc689dfd64012604c9c7
816d72a16c3f5fcdc0e86e7c03280b1c69b586ce0cd8aec722cc73a5d3b730310bf7dfebdc77ce5d94bbc369dc18a2f7b
07bd505ab0f82224aef09fdc1e5063234255e0b3c40a52e9e8ae60898eb88a766bdd788fe9493d8fd86bcdd2884d5c062
16c65469e5":16:"10001":"d5dcd27c74e040ea86f106b63d3275fa7b7e98d2dd701f38ec15fc7301b72df127f6d3bd557
1253a0b9e0e719d7d522893896941a1aeccc697912282b5308d829b91905b5dd7b7e1b8fe27e2bd4003b09dfe7fe295f
8a43c076c0cb52f2aac067e87de7ffe3a275d21a870c3dfc9b1d06d7f018667de9eb187bdf53d282e5d8b":0

RSA
PKCS1 Verify v1.5 CAVS #14
depends_on:MBEDTLS_SHA512_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"4ce61930c79dc017c2dea0c5085d73a3b0e4a6f341e9a5061a6658af11e5edf95bdad915ac
3619969e39bee15788a8de667f92f4efc84f35082d52d562aa74e12cc7f22d3425b58f5056d74afcf162cd44e65b9ee510
ff91af094c3d2d42c3b088536d62a98f1c689edcf3ea3fc228d711c109d76ae83d82d6a34dcfbad563cf":MBEDTLS_RS
A_PKCS_V15:MBEDTLS_MD_SHA512:1024:16:"e28a13548525e5f36dccb24ecb7cc332cc689dfd64012604c9c78
16d72a16c3f5fcdc0e86e7c03280b1c69b586ce0cd8aec722cc73a5d3b730310bf7dfebdc77ce5d94bbc369dc18a2f7b0
7bd505ab0f82224aef09fdc1e5063234255e0b3c40a52e9e8ae60898eb88a766bdd788fe9493d8fd86bcdd2884d5c0621
6c65469e5":16:"10001":"27280b92eab5cbf0d787ff6fa6b0151d6610adfd25116113f2f186f3f8d39736d91ae510ec2b
d96f2de135aefda79178138696dcc6d302e4a79ddabbe16e39ab96075776afce863e84a2e6013cb457e4047e22d43f67b
f64ae5e1d844a7c12ac696efbb3cda7c0e0aca71f8a7ada9a0547bfaefe1ba2e04058c672c803720dd9":0

RSA
PKCS1 Verify v1.5 CAVS #15
depends_on:MBEDTLS_SHA1_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"224ecd3b630581da948216366c741015a9723c5ea43de67e28454d0a846f54a6df167a25c

c500cf21f729aaefed6a71a3bdba438e12e20ad0c48396afe38568b70a3187f26098d6ac649a7c7ea68ed52748e712522
5102216236a28f67753b077cfd8d9198b86b0b331027cb59b24b85fd92896e8f2ff5a1d11872c2e6af6ae2":MBEDTLS
_RSA_PKCS_V15:MBEDTLS_MD_SHA1:1536:16:"a59d9b7269b102b7be684ec5e28db79992e6d3231e77c90b78
960c2638b35ef6dbdac1ac59e7249d96d426e7f99397eabc6b8903fe1942da580322b98bafacd81bb911c29666f83886a
2a2864f3552044300e60cedd5a8c321c43e280413dc41673c39a11b98a885486f8187a70f270185c4c12bc48a1968305
269776c070ef69d4913589a887c4d0f5e7dd58bd806d0d49a14a1762c38665cef4646ff13a0cd29c3a60460703c3d051
d5b28c660bffb5f8bd43d495ffa64175f72b8abe5fddd":16:"3":"1f7938b20a9cd8bb8ca26bad9e79ea92373174203f3ab
212a06de34a9a3e14e102d19a8878c28a2fc8083a97c06b19c1ae62678289d5d071a904aed1d364655d9e2d16480a6fd
18f4c8edf204844a34d573b1b988b82d495caefd9298c1635083e196a11f4a7df6a7e3cc4db7b9642e7682d22ec7038c3
bad791e1365fe8836976092460e6df749dc032baf1e026684f55936beb9369845c53c3d217941c1f8d8f54a32333a4c04
9c3f2d527125778032f5d390040d1d4cce83dc353ce250152":0

RSA
PKCS1 Verify v1.5 CAVS #16
depends_on:MBEDTLS_SHA256_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"6ecc722d233dad1aca45e6bc3e1a0b99fb1f89c0ec63bc657e6aaacbf931f267106cff42b71
2819f341b1ede798964a0b1a5032c198b391111e88d0d7303c02e23fa0137e74e604579a285b2dbc0a23aebdda65c371
eb403125bd366e822e72dceffe0d55dfa3155c16283020dc9abb0d150da1aef251484aa49e49e00974dac":MBEDTLS_
RSA_PKCS_V15:MBEDTLS_MD_SHA224:1536:16:"a59d9b7269b102b7be684ec5e28db79992e6d3231e77c90b7
8960c2638b35ef6dbdac1ac59e7249d96d426e7f99397eabc6b8903fe1942da580322b98bafacd81bb911c29666f83886
a2a2864f3552044300e60cedd5a8c321c43e280413dc41673c39a11b98a885486f8187a70f270185c4c12bc48a196830
5269776c070ef69d4913589a887c4d0f5e7dd58bd806d0d49a14a1762c38665cef4646ff13a0cd29c3a60460703c3d05
1d5b28c660bffb5f8bd43d495ffa64175f72b8abe5fddd":16:"3":"339dce3a1937669d9fb14c4f652378861fd5adc4da88
eaf833b16020b55a24ddc83b7ae3395a9a49b426bb9a4170cb765b02652faa9594b457aeefdae4f802e93d8e65c687ddc
723701465a5ef19249ed5d2617b5121c58557b34eb99a663bbcf4453a6e1db5d88723de449fcf58ca8ef514daf08cfdc7
1be155bb3d0724df0c0a6fd5aa7737433cc376640b9b8b4c7ddd09776bae0245729cddb56e36f28edad6aecaed0821ec
8d843a96348e722bf0a84cf060a793a2179f054138f907d0c3":0

RSA
PKCS1 Verify v1.5 CAVS #17
depends_on:MBEDTLS_SHA256_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"72f0b1ae27e1f5e5bfa15ded204c2c54b47b2420750a3eb5471f9ff98b67c8b5f1a30d3f8d6
448562e12ce4deb33a26cfeeae993d6be9e20679d8713c5216870f11276e5f22b0ead2821a7b4dee106fc1e19b13fc9fba
5d6e73e4bd93b65a9881a43d5e97ebfb0b357d5d06b21ddbecdbb10626d7748bb9e6e07d49316bbf3c4":MBEDTLS_
RSA_PKCS_V15:MBEDTLS_MD_SHA256:1536:16:"a59d9b7269b102b7be684ec5e28db79992e6d3231e77c90b7
8960c2638b35ef6dbdac1ac59e7249d96d426e7f99397eabc6b8903fe1942da580322b98bafacd81bb911c29666f83886
a2a2864f3552044300e60cedd5a8c321c43e280413dc41673c39a11b98a885486f8187a70f270185c4c12bc48a196830
5269776c070ef69d4913589a887c4d0f5e7dd58bd806d0d49a14a1762c38665cef4646ff13a0cd29c3a60460703c3d05
1d5b28c660bffb5f8bd43d495ffa64175f72b8abe5fddd":16:"3":"8117a6897e14c183737661cf5741350a84ae00495cd
9ee8fb033582e559f79701ab424706660515ee5821a69a6850647ec641676a625d1a3899932aaa52161fbc0c0a825db8
2fde0585b3c9b9c16de43e26da6a30fe5a601dae68bded1e29ec34557b5f6962efb10b9450d6f096655f68e8499cfa16a0
adeb9075e7b91851fef84243132d08273d35d01ad89c17e1e6e4deaf1cb233050b275fa9d2cae57e9e1a0e23139267040
aa39b6abd8f10fa1cec38ce2183573ddc11626fc262e1a0ced":0

RSA
PKCS1 Verify v1.5 CAVS #18
depends_on:MBEDTLS_SHA512_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"f80c94a2b53736978adf041886ad97ab2aeb9e91c08bd4eeef6b2f2b8dd75a99b45066571

88bbd7597bd5759121630627c8bf9cc30d90dd488c7a81cabab5350a62fa30abf5523f305b98f2c2c1743ec980cf26ab8
219bfd9505b981ab1abbfef733b384519d5259fc5c14577cb6b88fa7f6f332ff6a65b23faecc24342c78e9":MBEDTLS_
RSA_PKCS_V15:MBEDTLS_MD_SHA384:1536:16:"a59d9b7269b102b7be684ec5e28db79992e6d3231e77c90b7
8960c2638b35ef6dbdac1ac59e7249d96d426e7f99397eabc6b8903fe1942da580322b98bafacd81bb911c29666f83886
a2a2864f3552044300e60cedd5a8c321c43e280413dc41673c39a11b98a885486f8187a70f270185c4c12bc48a196830
5269776c070ef69d4913589a887c4d0f5e7dd58bd806d0d49a14a1762c38665cef4646ff13a0cd29c3a60460703c3d05
1d5b28c660bffb5f8bd43d495ffa64175f72b8abe5fddd":16:"3":"6b49553ed964ae196a41ea281f4d2a250ce7d1e7434e
45cf6a82f7bed17554f39c3f0241e0364702fcb87475eb0c0839ffd2180890fa05b4bbf31bbfa4bf5119dea0c9f88e1e961
7fcdadabc6fa1945136cc66e039b905d78ed365c5806d38aec88b3edfb86c05ff446dbfd51d7cd75cbf8d3b85154c7837
65386f51637532221f52429db5612dcc034968bb8feab7dc6f5ed1f2feb557f6dd49c980296117be2c4195ec7b6101ea7
67df9d16a56fc9709b49308a54dab63dbc4d609f959ce17":0

RSA
PKCS1 Verify v1.5 CAVS #19
depends_on:MBEDTLS_SHA512_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"4eb97094bb42aaa58b040bd06a8f324396b9eca9e39359b7039c4a010434ee131a53aebd9
f7a55ae58ea7444fa1505a3ec524e054fd408513cddc1ee4c2f7fd95ec4a6f594be1ba39fa1aa933dc0a5dafff5ce4450957
7ebb3a3e8084c44010aa27321e5a3f646ade99175633b795c0f570b360eeebeefaef15788f80b5cbecd":MBEDTLS_RS
A_PKCS_V15:MBEDTLS_MD_SHA512:1536:16:"a59d9b7269b102b7be684ec5e28db79992e6d3231e77c90b7896
0c2638b35ef6dbdac1ac59e7249d96d426e7f99397eabc6b8903fe1942da580322b98bafacd81bb911c29666f83886a2a
2864f3552044300e60cedd5a8c321c43e280413dc41673c39a11b98a885486f8187a70f270185c4c12bc48a196830526
9776c070ef69d4913589a887c4d0f5e7dd58bd806d0d49a14a1762c38665cef4646ff13a0cd29c3a60460703c3d051d5
b28c660bffb5f8bd43d495ffa64175f72b8abe5fddd":16:"3":"2b8b794a8621d492eec18a4efd239e0e077c89340a34b0f
dbf467f2bf3112c7f33d00ee736f2988af8569c1a74891efbefa839e295fffdf4d908c1ede61a861a4d24b154a09d1b3f92
3fd2bb7906994cf82a97da285bf48e61f90cc3596f9350ab9b66a216ffca323195bb213f5a77fe8c697475595a1857dbee
58128cbf1be7cb220229ce52766fefd88cc129ad5cbbdcd31fb4eede6c4fdd3193a9aaaa54362bcea4082981d9b7c4048
3814828f3297d95ad933c76f31c47e37a93ffaf0d4a":0

RSA
PKCS1 Verify v1.5 CAVS #20
depends_on:MBEDTLS_SHA1_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"a3edb0f52c6166d7b76e71634761f402337c3e9667549d00cd7877e6055396b35c54c4dff
c4c987060178fc10b7e5e827a5c870057002ba6efd31fc4e63a429029be0d6b256b6b653775cb026322743f48e319d05
3c4aeac34077acb8e0c6c2ef375b2210f8788bd23d24eb0b614de41875b1c8ec56acf18825eaf826691be96":MBEDTL
S_RSA_PKCS_V15:MBEDTLS_MD_SHA1:1536:16:"a59d9b7269b102b7be684ec5e28db79992e6d3231e77c90b7
8960c2638b35ef6dbdac1ac59e7249d96d426e7f99397eabc6b8903fe1942da580322b98bafacd81bb911c29666f83886
a2a2864f3552044300e60cedd5a8c321c43e280413dc41673c39a11b98a885486f8187a70f270185c4c12bc48a196830
5269776c070ef69d4913589a887c4d0f5e7dd58bd806d0d49a14a1762c38665cef4646ff13a0cd29c3a60460703c3d05
1d5b28c660bffb5f8bd43d495ffa64175f72b8abe5fddd":16:"10001":"180630d2f4dc91ddb1159978e278cda7ac4b178
e82477f9770c4d2e1c5017d2f222348658044c1be4cda24ce3c9ba3d423536a39bf60324c1b30eabdad700b0982e5807
2f7e18216e7e4c07e17674ec3eabcfbafce317d2f539f129902d80031ca201a8b325629a96ca4a70b51294c2fddd1d0aca
1537d7d8b780e1e62d34be2f98104d876a4990396c8628e6498d9651f468bdf1139664eabe9166efbe909bf87d7305d5
f60f1acc3599ed339fcf4e009fbad4059af1a50264cb0a4ec1d23f3":0

RSA
PKCS1 Verify v1.5 CAVS #21
depends_on:MBEDTLS_SHA1_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"ac58fd024208d7f045d81a56cd55aad40ab86b0d216ab55136c7027aca23ea13480a52c0d

acce0d98139b25965aa4ff76a41dd92037195d24bc0750d52cb3467b48b7b3e71d852c5f82bd9ee85a8388ead5cd8bc38c3d4792e8daa9734a137d31963e245ad3217fad235f7dfd5584de0fe91c4526568588e08b60bdf1badd99f":MBEDTLS_RSA_PKCS_V15:MBEDTLS_MD_SHA1:1536:16:"a59d9b7269b102b7be684ec5e28db79992e6d3231e77c90b78960c2638b35ef6dbdac1ac59e7249d96d426e7f99397eabc6b8903fe1942da580322b98bafacd81bb911c29666f83886a2a2864f3552044300e60cedd5a8c321c43e280413dc41673c39a11b98a885486f8187a70f270185c4c12bc48a1968305269776c070ef69d4913589a887c4d0f5e7dd58bd806d0d49a14a1762c38665cef4646ff13a0cd29c3a60460703c3d051d5b28c660bffb5f8bd43d495ffa64175f72b8abe5fddd":16:"10001":"a142b0d9456f8f4772675265a08613a66c416bd1ae712975c69d9ca5fb8c1be9c24359a04fd15460bf6136a8a11f13e3ce2de2171524f10cb715f0d71e3db15281ab99eadbe86cf8c5c518162c638ef27a4f7bfb4a1a3873f3c384a5b1c3b4966c837b9d8d192ac34e03943b7ae191355aa1ff3b9cd041bb2668f1f81cf0d015b3d3608cd9ac79398212c0f132f1bd45d47768b999fcf3c05fe2069593ceecedc851a7fc465abcfef0fabba9b9460153f6ba8723a5c6e766c83a446aef3ee327":MBEDTLS_ERR_RSA_INVALID_PADDING

RSA
PKCS1 Verify v1.5 CAVS #22
depends_on:MBEDTLS_SHA256_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"027f767928a5821e2723d6f36c43e6b498b6f0b381852571794a096bd49f1c36a4d7bacec7ec402c24b970163169173bb930ec7fdc39bc9457dfc4ca051f5f28a64de1bbe007c22e8368ff9b117dbda17efd2fb73434bbbf5a4158df56813b8c904bb2e779de504dcd974a291568210d6f85810291606a1c0cd88d51ceadf98a":MBEDTLS_RSA_PKCS_V15:MBEDTLS_MD_SHA224:1536:16:"a59d9b7269b102b7be684ec5e28db79992e6d3231e77c90b78960c2638b35ef6dbdac1ac59e7249d96d426e7f99397eabc6b8903fe1942da580322b98bafacd81bb911c29666f83886a2a2864f3552044300e60cedd5a8c321c43e280413dc41673c39a11b98a885486f8187a70f270185c4c12bc48a1968305269776c070ef69d4913589a887c4d0f5e7dd58bd806d0d49a14a1762c38665cef4646ff13a0cd29c3a60460703c3d051d5b28c660bffb5f8bd43d495ffa64175f72b8abe5fddd":16:"10001":"0676e64daaa18f4af46e9dfbe234db389b8a527b0fe1db97eb7f404e3155226cba70d318800f83160fa1aa19916e5c09f079331079f18cb8ab1a4b884cb28501824974f683ed2b9babae9f8c15bea30802805c6b2152119764811bbf5f3994d2e97fa2fe8c5ab15a23c14d7ae56be00eaa8bc26678481ff5ba59b0acfb0e43341bff9fc638e5625480a73dbc5d8d13bd2b9e64037c6b79df0c60869980c6a22ec46f80fb859cb4ee5d2032ac1fe538cfd85c70a7f33b4af50a93395917c2cfb6":MBEDTLS_ERR_RSA_INVALID_PADDING

RSA
PKCS1 Verify v1.5 CAVS #23
depends_on:MBEDTLS_SHA256_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"06dcd9d4c056b6a45b9ed2ae5f6c1cfa43aae06fe01ee098264aa7a80e901abbcf9a505e55f9a352ef0c078d48249b8298e57ea21bf0e423c3bf69002acfa541ca05007c704bc79cee7a80e1107c7b28d2b2aa6dd093b28efe9642519952a4a95ee49235f9924a0ac0aee5b2a1bce47459d70cd6e75074614199dca44561407c":MBEDTLS_RSA_PKCS_V15:MBEDTLS_MD_SHA224:1536:16:"a59d9b7269b102b7be684ec5e28db79992e6d3231e77c90b78960c2638b35ef6dbdac1ac59e7249d96d426e7f99397eabc6b8903fe1942da580322b98bafacd81bb911c29666f83886a2a2864f3552044300e60cedd5a8c321c43e280413dc41673c39a11b98a885486f8187a70f270185c4c12bc48a1968305269776c070ef69d4913589a887c4d0f5e7dd58bd806d0d49a14a1762c38665cef4646ff13a0cd29c3a60460703c3d051d5b28c660bffb5f8bd43d495ffa64175f72b8abe5fddd":16:"10001":"5e08f399258e6de075b67a0a6a822ceb21b1eb7a0342eca6a4295739f644547dee3456243cf32bd6ea6f357c88632508457130f3dae04f7806efaed43d1d501e16c961dfbd6c71a42b480e95c7027f8275063d05a9aac3eef0520867b9896ebe8ec358f7d121beb4e61ddfdc3dcd835dfe265f2ba68d300ef566ed1284f9f3d7b1af363ed47bfa2e5f0492925444df7e5fcb1e79e690c746117650b543a5e82c39553552f0f44e617b5cf773c533050f4129e893ac22af69b1eb9afb4b5ba5f5":0

RSA
PKCS1 Verify v1.5
CAVS #24
depends_on:MBEDTLS_SHA256_C:MBEDTLS_PKCS1_V15

mbedtls_rsa_pkcs1_verify:"1240028c6d7ab3992ada0e5ca55ee4f3d62f8de575302d5861d73685423c2e6a6d6fb3be0
90fbc2a701821b6d8fd5e8233f794b6549cd0bb52b390ac31478307bffa91a9bd9c1bf93ffc846356fef008ebee4bb3ee1
48e0fb1893d188e4934d0d088a433d14a596c5f2e3e49648a22edc6bdbcc58dc1edbd440046b3a169ca2b":MBEDTLS
_RSA_PKCS_V15:MBEDTLS_MD_SHA256:1536:16:"a59d9b7269b102b7be684ec5e28db79992e6d3231e77c90b
78960c2638b35ef6dbdac1ac59e7249d96d426e7f99397eabc6b8903fe1942da580322b98bafacd81bb911c29666f8388
6a2a2864f3552044300e60cedd5a8c321c43e280413dc41673c39a11b98a885486f8187a70f270185c4c12bc48a19683
05269776c070ef69d4913589a887c4d0f5e7dd58bd806d0d49a14a1762c38665cef4646ff13a0cd29c3a60460703c3d0
51d5b28c660bffb5f8bd43d495ffa64175f72b8abe5fddd":16:"10001":"a003ae9cf0704d58763b214f20446ecc4099c56
6f25384e28d0dd6540c58705fc8d0bfe1ceaa06096ed1e230146edb82056e39e6727abec09f25e44079b6ce1ca2c6a540
dec7aa34444d7d435f41e5fca9b0bba62759ae2780638e5160e031bb60409c2e85674ac7a776b444b37b9d7f4dbaa557
e88b8562a584f2dbe90729b241aede95dfcc7e05b10deef06255cb89f0e7ccff23354818756a1f8bb9f00fd18f6cd22ca1b
4bfc38027562bb37562c77c7883b5d735170d75521195fd3f2bd3":0

RSA
PKCS1 Verify v1.5 CAVS #25
depends_on:MBEDTLS_SHA512_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"67922a8b9cbc95cf7c555ff2d73cfc62ee04c3f0df9bfc8f64293a58bd3bebd2eb212d711f9
4e35c729d0873d6b244914d21bd0e59b23089b38740e43f480e8f407d090ac93b08a57403968b55e78cfe31eee6e4ecb
acf834168fe89b6b8454fce6e675e80f82b33e850ae3f3d24fd320335e37981fd000576941b4f08d4ba99":MBEDTLS_
RSA_PKCS_V15:MBEDTLS_MD_SHA384:1536:16:"a59d9b7269b102b7be684ec5e28db79992e6d3231e77c90b7
8960c2638b35ef6dbdac1ac59e7249d96d426e7f99397eabc6b8903fe1942da580322b98bafacd81bb911c29666f83886
a2a2864f3552044300e60cedd5a8c321c43e280413dc41673c39a11b98a885486f8187a70f270185c4c12bc48a196830
5269776c070ef69d4913589a887c4d0f5e7dd58bd806d0d49a14a1762c38665cef4646ff13a0cd29c3a60460703c3d05
1d5b28c660bffb5f8bd43d495ffa64175f72b8abe5fddd":16:"10001":"2c6b301852cc55a993a933e2c080eb9dabfe19e9
dc3571066caeabed1492d3501cd838de1c01784932df7a5ad5bbfb48c78f53a45f76e9812d046f23bd968495ef7e981e5
add4acfc538fe33a5205de74bb37d3d9b6b87b2d174e85a73f216fd67d5738fc469dff7ea6b852e8dd08bc8df03659737
2d4d51185e6f47a45fbe1b9bdb06a4018783425ec95294de41f27235ad3b3263a890b8b62b17410a9bb08673393ff205
a866ee2057e99c6517c6bbc84f8d87717b83d6f64de7ee215e1e8d":0

RSA
PKCS1 Verify v1.5 CAVS #26
depends_on:MBEDTLS_SHA512_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"1428b4a449698a994ef84c46a517c3aa6359c48e4264ef65f1f69d77ae26133e17edfc103d
e416fffb4f2bfe865b434544a418f6e2faca00a165d443f0663ff64080154614f7194057d8b5f1f33934cc9fc2314cf86d4f
dad4892bf0d3058f7f37ebe98ef52bfb240b9ad369153afe081bbcf9d7ae43e8ba336b8ac57e8a6da0":MBEDTLS_RSA
_PKCS_V15:MBEDTLS_MD_SHA512:1536:16:"a59d9b7269b102b7be684ec5e28db79992e6d3231e77c90b78960
c2638b35ef6dbdac1ac59e7249d96d426e7f99397eabc6b8903fe1942da580322b98bafacd81bb911c29666f83886a2a2
864f3552044300e60cedd5a8c321c43e280413dc41673c39a11b98a885486f8187a70f270185c4c12bc48a1968305269
776c070ef69d4913589a887c4d0f5e7dd58bd806d0d49a14a1762c38665cef4646ff13a0cd29c3a60460703c3d051d5b
28c660bffb5f8bd43d495ffa64175f72b8abe5fddd":16:"10001":"8e10a1ae470e6e57a8d234185f78fdb600cc636c4156
5a9f3694a84ae102f6251984f54d11a7785fdcfdfaf80a821e05d57ef6b8edc03d9076755779322fd53eb98c805da77dc9
316744e393c2fecd291a7e6043b1ca89fd8248f661e1d53110211b91edb41b31e848cde1115d8afd9963ebcc36aff5a27
085949f0781bc69167c140ecfe71c44aacaf4123e557eaf2b528c6d0ea875b4ceefa942fe338af8df10562c438af04cd752
1da912b3e3899cef0d75722161be6abed5e4e9009dbf40":0

RSA
PKCS1 Verify v1.5 CAVS #27
depends_on:MBEDTLS_SHA1_C:MBEDTLS_PKCS1_V15

mbedtls_rsa_pkcs1_verify:"4871adc05f6b3ecf296680b0dd8d86715b0d5264c064008037dc410512520b5f193c8f4d2
1eb6c42e10d220c0275c9b3751f03a4096e2f0e3db9df8d52068c06a51589d23ca1361e9fe27691e95663301ec1407fbf
73aee99cc92362eaf6994b95038396d815052a0aef6489bbb7bcb0fffdf13f0af9e7d9fd14f6ce00ab98f7":MBEDTLS_R
SA_PKCS_V15:MBEDTLS_MD_SHA1:1536:16:"a59d9b7269b102b7be684ec5e28db79992e6d3231e77c90b7896
0c2638b35ef6dbdac1ac59e7249d96d426e7f99397eabc6b8903fe1942da580322b98bafacd81bb911c29666f83886a2a
2864f3552044300e60cedd5a8c321c43e280413dc41673c39a11b98a885486f8187a70f270185c4c12bc48a196830526
9776c070ef69d4913589a887c4d0f5e7dd58bd806d0d49a14a1762c38665cef4646ff13a0cd29c3a60460703c3d051d5
b28c660bffb5f8bd43d495ffa64175f72b8abe5fddd":16:"11":"180caf03781b391aacebe5b3f5e1d3b01c68a00df4ecfb6
c4bf14217aed7cfca0adac099ec1d6e1f0b43b09b86788533fee6691d773807af0df6cc3bbdde3cf34bf5b848fa59c8bc10
227cc3eba3452a85e0520fccdb2d8d32dd99672d302756a2d7f7f2693db3a48be17bd34d9d891f4ba44449c5bad1de91
b788f524500a7703cccbaa77b9fe8791f5c8aa7b8f055336f28fcfc01733712e33cfb3d33fe71ddb9ced2a31931ec38007f
5ad4a0d19acc428124b0e5ee6e0746fb33c1a4d90c8":0

RSA
PKCS1 Verify v1.5 CAVS #28
depends_on:MBEDTLS_SHA256_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"3bba64de38438a71b95ab9c94539d5870c1fb08d7a9937600c00e9d063438edc97e625d0
cd4b1eb00c31c9d94c7a0fe6d03160d1b6cbec5acdad16ada6ef253fee603df9faca8f98a477cc5456f3dfbf6414dbf19f3
832e227ce291780188881e82e96a2e84744f12a34a9808a2daedc6fd00b345c6772bec26a095719451e6a":MBEDTLS
_RSA_PKCS_V15:MBEDTLS_MD_SHA224:1536:16:"a59d9b7269b102b7be684ec5e28db79992e6d3231e77c90b
78960c2638b35ef6dbdac1ac59e7249d96d426e7f99397eabc6b8903fe1942da580322b98bafacd81bb911c29666f8388
6a2a2864f3552044300e60cedd5a8c321c43e280413dc41673c39a11b98a885486f8187a70f270185c4c12bc48a19683
05269776c070ef69d4913589a887c4d0f5e7dd58bd806d0d49a14a1762c38665cef4646ff13a0cd29c3a60460703c3d0
51d5b28c660bffb5f8bd43d495ffa64175f72b8abe5fddd":16:"11":"8c846e75e32ce5f9964bdd8f6dcf1d2996a646b233
bcf1bd6394e13e856691b89bedd18290a0f9f7c90dca307271b3108e795340490513b25e6789e93722c65ec064b4c434
57295a31d1f07dd605e133fd6eaafc58cda132df2939f5f693e0205af34550afaa137f3e482885e50dfb48333a15c0821e
7a19642acdddc6fea3c7487c691246a2b083dac439889d5ae741b7e08c47937530b4b069f1a260cd07fe4a0ddd530ab1
1534fb805e9b562118ee0e97932966008aadfc83f3b8a10de8ee":0

RSA
PKCS1 Verify v1.5 CAVS #29
depends_on:MBEDTLS_SHA256_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"f7857ce04bf4292ea1755f9e587822372f4dcdf10bddfc0ff498a8af60ae94a0b482e873085
c1cd52a5d181ce6b99a1f8520d74b947d65f3e7e358e8ddc4ac4ae465e39d408eee1f09865159733f83f553cd93cfde1c1
14fb3e32cf51cd418359016b3867df467b645d752808671a4609f3c49a67023c9ca617e6cffa544a10a":MBEDTLS_RS
A_PKCS_V15:MBEDTLS_MD_SHA256:1536:16:"a59d9b7269b102b7be684ec5e28db79992e6d3231e77c90b7896
0c2638b35ef6dbdac1ac59e7249d96d426e7f99397eabc6b8903fe1942da580322b98bafacd81bb911c29666f83886a2a
2864f3552044300e60cedd5a8c321c43e280413dc41673c39a11b98a885486f8187a70f270185c4c12bc48a196830526
9776c070ef69d4913589a887c4d0f5e7dd58bd806d0d49a14a1762c38665cef4646ff13a0cd29c3a60460703c3d051d5
b28c660bffb5f8bd43d495ffa64175f72b8abe5fddd":16:"11":"9677300bbee003be3c445634f8ed5beb152b63f46f84cf
5a8e721e0fafe8f3f7e99a6d50741f23f449d3026da3e8a7ac36be99ab44831803486ae552f7aa01f075287829b231d2d0
840908e09081ae177ed888fe46a9d937a0871eb5d52ec541c8411c4cbf7efea6ca213b12cea513b0739eedca7c9473e10
a7796936f4eaa0c5d3a9013ca5536781ac68eb2ca5779144de23da2e9875114aca885b3219dfc292d73940c5992ea3c4
882889e7543430652860e441a01a45d9f4005a012421493":0

RSA
PKCS1 Verify v1.5 CAVS #30
depends_on:MBEDTLS_SHA256_C:MBEDTLS_PKCS1_V15

mbedtls_rsa_pkcs1_verify:"ca312774f2756ac2019f213a01a63c9a0b4a49ccafecf25e97a4c632668e3c77e664f4d7635
241f25205e50c37061b02c546db8346fa597c3da8cfd44a827c5a4ff4ecfcd1797b39a1b215d9bbb93fdb6eb35bafbda42
7a5068888a6e19f86224b0897490491207e35ce39085668b10b4fb851b7dd9465c03869790ef38a61b5":MBEDTLS_
RSA_PKCS_V15:MBEDTLS_MD_SHA256:1536:16:"a59d9b7269b102b7be684ec5e28db79992e6d3231e77c90b7
8960c2638b35ef6dbdac1ac59e7249d96d426e7f99397eabc6b8903fe1942da580322b98bafacd81bb911c29666f83886
a2a2864f3552044300e60cedd5a8c321c43e280413dc41673c39a11b98a885486f8187a70f270185c4c12bc48a196830
5269776c070ef69d4913589a887c4d0f5e7dd58bd806d0d49a14a1762c38665cef4646ff13a0cd29c3a60460703c3d05
1d5b28c660bffb5f8bd43d495ffa64175f72b8abe5fddd":16:"3":"a202c33eb831b9d8e818b6c3bcdb42818e1d9c22a06
ddd73a17a21e49d18cda44df349a066477cae068e1a5d2b518b0885e889ef796ca9e6f42a69ac755b8a6405fbaef93fe01
30d98de35d689addfee3eecd26658903f774bda481c3f40ee0e9569a3c3e2da7ad576c7de82159d933e36fa29cfef99367
005e34ab5082d80f48276d37dabc88dbb023bd01585329d2ccf417f78ec508aaa29751007d31f1669296b981d44c8fa9
9130c5df7a071725b496859314aaf9baf0ebc780355914249":MBEDTLS_ERR_RSA_INVALID_PADDING

RSA
PKCS1 Verify v1.5 CAVS #31
depends_on:MBEDTLS_SHA512_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"2abe079077290ceb6c80ac5c61062ce8da814b1fb99a1a9fb2860ed900e6541856ec64bf19
c0d9d1cc2280b7cc50af3e3d2ad8e044945d44761ca60891dd72bd6aa26a33274ffcf7ae7d661b5e651135fcff21aaf06b
4a2db18fe5827e0243884f2841760b9f1c65fbda870f7f0cfbd6ff484f0825e688614928f2d12d1e7080":MBEDTLS_RS
A_PKCS_V15:MBEDTLS_MD_SHA384:1536:16:"a59d9b7269b102b7be684ec5e28db79992e6d3231e77c90b7896
0c2638b35ef6dbdac1ac59e7249d96d426e7f99397eabc6b8903fe1942da580322b98bafacd81bb911c29666f83886a2a
2864f3552044300e60cedd5a8c321c43e280413dc41673c39a11b98a885486f8187a70f270185c4c12bc48a196830526
9776c070ef69d4913589a887c4d0f5e7dd58bd806d0d49a14a1762c38665cef4646ff13a0cd29c3a60460703c3d051d5
b28c660bffb5f8bd43d495ffa64175f72b8abe5fddd":16:"10001":"402631f3cddfb02cc4d9cb58ef1ab6726bd787a50e1
2e98567c9702bfdf47af85904aec5a2f6c5df9a10f08f90f93728eb090ae2ac21ded9f38faecd8195f3eb3d4107521b1cee
956e7a214245b038adae912fa35ec97cb3bdc41352e8aaff80173561284cb740f999a3cd6653a6c3d5a3f911a416f41e2
155083982c99eb5998a0a74d77f1ae999d901ee24a7f2c424179a3f92b07dc0b3498c1884e60677bee0175e810b426c4
ad008d2743cd19b00b33177bf8be3fed7f7406e1bce0c2ea3":MBEDTLS_ERR_RSA_INVALID_PADDING

RSA
PKCS1 Verify v1.5 CAVS #32
depends_on:MBEDTLS_SHA512_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"da9505809dc92cfd8e01a1857dde52df6677c40d98f4577c1659ca7d3e9f01f9a809065f51
b54fe2f9723fe2c9d1eea7397f2d5531d1c51c6ea100b028596bf9f24dd90be14eab58f07b4f24a35b073aeb29ecde4a6f
320237d7adbdc43d94f87e08866b95bbcac83dc7db3553a42400441f088e2bf6259539a2da8b5a74065f":MBEDTLS_
RSA_PKCS_V15:MBEDTLS_MD_SHA384:1536:16:"a59d9b7269b102b7be684ec5e28db79992e6d3231e77c90b7
8960c2638b35ef6dbdac1ac59e7249d96d426e7f99397eabc6b8903fe1942da580322b98bafacd81bb911c29666f83886
a2a2864f3552044300e60cedd5a8c321c43e280413dc41673c39a11b98a885486f8187a70f270185c4c12bc48a196830
5269776c070ef69d4913589a887c4d0f5e7dd58bd806d0d49a14a1762c38665cef4646ff13a0cd29c3a60460703c3d05
1d5b28c660bffb5f8bd43d495ffa64175f72b8abe5fddd":16:"11":"57edd0560df9840a25c28ff6d254e432395a5cd2d92
248b3b44d7eab0fc65b3c4e545a916a8e90ce89745119db9ec9799aa8890f5250fb589cfc12dac1b6e406a39bc3b36638
92da5354ba453cbd5e4c89bdce82d0ffe97052a03a5c3308819c1139ebc780c13cf6dc1477faf734abcb1db3fafaed6f22
885c9c0222ff5deacb8cc6d027f2e959c3075011b382e88c4b27b83b4f2e6fda022e331c3602d19f5ac7bccfe95ea1e93d
736dbd918ae5b1f468cd0b5b536a2f918d5e27a0757e75b7":0

RSA
PKCS1 Verify v1.5 CAVS #33
depends_on:MBEDTLS_SHA512_C:MBEDTLS_PKCS1_V15

mbedtls_rsa_pkcs1_verify:"d0cd038c65b3acca45822eaf91ea5176e82043268876dec0b62e2abd619023b7023abc67c6b823cfef5447b8772f985ff7910d6cc87e6c23688ac6de1fee40bbe2da1a92770de92adaa427ace02fee571a0a0176fceb0c8f3eb72dde839ab201395625f5c0db8641ce19d7711212dec61733262c6ce4476c025e67a3d5bc01f3":MBEDTLS_RSA_PKCS_V15:MBEDTLS_MD_SHA512:1536:16:"a59d9b7269b102b7be684ec5e28db79992e6d3231e77c90b78960c2638b35ef6dbdac1ac59e7249d96d426e7f99397eabc6b8903fe1942da580322b98bafacd81bb911c29666f83886a2a2864f3552044300e60cedd5a8c321c43e280413dc41673c39a11b98a885486f8187a70f270185c4c12bc48a1968305269776c070ef69d4913589a887c4d0f5e7dd58bd806d0d49a14a1762c38665cef4646ff13a0cd29c3a60460703c3d051d5b28c660bffb5f8bd43d495ffa64175f72b8abe5fddd":16:"11":"2f30629c1117d013bb36e6099dee931dcaf0a1032b07ec23e2b262898a8945e569c9573d81e22bb0a5f8a28b0d7b8ff01367dd7f089c68ed1daa11cf53a96ee91b38e6b839b6e90bea34d14b78f5d2c7629b68c5b4f2ecfff66b483b2233cb14f95df533c867a2b610aebcdbb7ea3109aaf2f5762ab3edc2571deccc7da0c9a5b443ca2b924c0f18de7bbb736a08fed3916795018a436a3ae62c85d554a53a6d48623908e06e7d275f4251d3b3bd530bd11e155dcf2b5c2adf030cdf931ae749":MBEDTLS_ERR_RSA_INVALID_PADDING

RSA
PKCS1 Verify v1.5 CAVS #34
depends_on:MBEDTLS_SHA512_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"59779fd2a39e56640c4fc1e67b60aeffcecd78aed7ad2bdfa464e93d04198d48466b8da7445f25bfa19db2844edd5c8f539cf772cc132b483169d390db28a43bc4ee0f038f6568ffc87447746cb72fefac2d6d90ee3143a915ac4688028805905a68eb8f8a96674b093c495eddd8704461eaa2b345efbb2ad6930acd8023f870":MBEDTLS_RSA_PKCS_V15:MBEDTLS_MD_SHA512:1536:16:"a59d9b7269b102b7be684ec5e28db79992e6d3231e77c90b78960c2638b35ef6dbdac1ac59e7249d96d426e7f99397eabc6b8903fe1942da580322b98bafacd81bb911c29666f83886a2a2864f3552044300e60cedd5a8c321c43e280413dc41673c39a11b98a885486f8187a70f270185c4c12bc48a1968305269776c070ef69d4913589a887c4d0f5e7dd58bd806d0d49a14a1762c38665cef4646ff13a0cd29c3a60460703c3d051d5b28c660bffb5f8bd43d495ffa64175f72b8abe5fddd":16:"11":"0b4d96f411c727a262d6d0ade34195b786035510611917d060f89add47b09dfe8715f4f9147d327dc25e91fe457e5d1a2f22cd8fe6fe8e29d2060658307c87a40640650fef3d4b289a6c3febc5a100b29a8b56623afb29fd3c13ea372bf3c638c1db25f8bd8c74c821beec7b5affcace1d05d056a6c2d3035926c7a268df4751a54bc20a6b8cfd729a7cba309ae817daccbef9950a482cf23950a8ca1d3a13ddb7d8d0f87ad5587d4d9ebe19fe93457597a7bdd056c2fd4cea7d31e4a0e595a7b":0

RSA
PKCS1 Verify v1.5 padding too short
depends_on:MBEDTLS_SHA1_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"AABBCC03020100FFFFFFFFFF1122330A0B0CCCDDDDDDDDDD":MBEDTLS_RSA_PKCS_V15:MBEDTLS_MD_SHA1:1024:16:"9292758453063D803DD603D5E777D7888ED1D5BF35786190FA2F23EBC0848AEADDA92CA6C3D80B32C4D109BE0F36D6AE7130B9CED7ACDF54CFC7555AC14EEBAB93A89813FBF3C4F8066D2D800F7C38A81AE31942917403FF4946B0A83D3D3E05EE57C6F5F5606FB5D4BC6CD34EE0801A5E94BB77B07507233A0BC7BAC8F90F79":16:"10001":"6edd56f397d9bc6d176bbe3d80946fc352ad6127b85b1d67d849c0a38cbde7222c5fafbb18dcef791178a8e15f5c8cd91869f8ca4b758c46ce3e229bf666d2e3e296544351bcb5db7e0004f6c0800f76a432071297e405759d4324d1cf1c412758be93a39f834e03dee59e28ac571ce2b0b3c8fe639979f516223b54027340a5":MBEDTLS_ERR_RSA_INVALID_PADDING

RSA PKCS1 Sign #1 (SHA512, 1536 bits
RSA)
depends_on:MBEDTLS_SHA512_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_sign:"59779fd2a39e56640c4fc1e67b60aeffcecd78aed7ad2bdfa464e93d04198d48466b8da7445f25bfa19db2844edd5c8f539cf772cc132b483169d390db28a43bc4ee0f038f6568ffc87447746cb72fefac2d6d90ee3143a915ac4688028805905a68eb8f8a96674b093c495eddd8704461eaa2b345efbb2ad6930acd8023f870":MBEDTLS_RSA_PKCS_V15:MBEDTLS_MD_SHA512:1536:16:"c8c67df894c882045ede26a9008ab09ea0672077d7bc71d41251

1cd93981ddde8f91b967da404056c39f105f7f239abdaff92923859920f6299e82b95bd5b8c959948f4a035cbd693ad83
014294d349813d1ad57911a6355d0731fe3a034e9db":16:"f15147d0e7c04a1e3f37adde802cdc610999bf7ab0088434
aaeda0c0ab3910b14d2ce56cb66bffd97552195fae8b061077e03920814d8b9cfb5a3958b3a82c2a7fc97e55db5978b47
a922156eb8a3e55c06a54a45d1670abdfb995489c4d0051":16:"bd429bb7c3b00bbea19ba664c0f8172d1a73c3cfa05e
2ed656d570c1590918bb7e372ed25e2cd71395ba0a9b1a30f3ee012ffb0546cab8e3581fe3e23f44ab57a8aee9717e71a
936a580fa8572d450fb00339a6f6704b717df0c149a465bab768c61500cd93b61113ff3e4389167f7b2c8e3c0da2d4765
286bee555b0bcb4998f59b14fad03180a17c8b4f69bcd1234f4ae85950137665ac2ba80b55cc9b1aafb454b83771aa755
acd2a00e93ddb65e696dbed8bdca69fb5e0c5c2097b9cfe4b":16:"3":"93b6fa99485c116ca6efdd4202ea1cf49f4c6345f
ae692584413743ce5b65510e8e4690aee9a19ea1ff10d57f22aa3548d839f28a8525a34354e9e58e0f3947e056ce2554e
21bf287e220b98db3b551258cd42b495e5d1a3bbc83c9d1a02f2a300ef6d866ea75108e44ebb3e16b47df2f6de28feb2b
e3874dbbf21599451082d86e9f2f462575a8185c69aa1f1fcb6a363c5d71aeba2103449eaf3845285291148d5f78d1646
b8dc95cbcc4082f987d948b0e7d4e80b60595f8a7517584e1643":0

RSA
PKCS1 Sign #1 Verify
depends_on:MBEDTLS_SHA512_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"59779fd2a39e56640c4fc1e67b60aeffcecd78aed7ad2bdfa464e93d04198d48466b8da744
5f25bfa19db2844edd5c8f539cf772cc132b483169d390db28a43bc4ee0f038f6568ffc87447746cb72fefac2d6d90ee31
43a915ac4688028805905a68eb8f8a96674b093c495eddd8704461eaa2b345efbb2ad6930acd8023f870":MBEDTLS_
RSA_PKCS_V15:MBEDTLS_MD_SHA512:1536:16:"bd429bb7c3b00bbea19ba664c0f8172d1a73c3cfa05e2ed656
d570c1590918bb7e372ed25e2cd71395ba0a9b1a30f3ee012ffb0546cab8e3581fe3e23f44ab57a8aee9717e71a936a58
0fa8572d450fb00339a6f6704b717df0c149a465bab768c61500cd93b61113ff3e4389167f7b2c8e3c0da2d4765286bee
555b0bcb4998f59b14fad03180a17c8b4f69bcd1234f4ae85950137665ac2ba80b55cc9b1aafb454b83771aa755acd2a0
0e93ddb65e696dbed8bdca69fb5e0c5c2097b9cfe4b":16:"3":"93b6fa99485c116ca6efdd4202ea1cf49f4c6345fae6925
84413743ce5b65510e8e4690aee9a19ea1ff10d57f22aa3548d839f28a8525a34354e9e58e0f3947e056ce2554e21bf28
7e220b98db3b551258cd42b495e5d1a3bbc83c9d1a02f2a300ef6d866ea75108e44ebb3e16b47df2f6de28feb2be3874d
bbf21599451082d86e9f2f462575a8185c69aa1f1fcb6a363c5d71aeba2103449eaf3845285291148d5f78d1646b8dc95
cbcc4082f987d948b0e7d4e80b60595f8a7517584e1643":0

RSA
PKCS1 Sign #2 (SHA256, 2048 bits RSA)
depends_on:MBEDTLS_SHA256_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_sign:"59779fd2a39e56640c4fc1e67b60aeffcecd78aed7ad2bdfa464e93d04198d48466b8da7445f
25bfa19db2844edd5c8f539cf772cc132b483169d390db28a43bc4ee0f038f6568ffc87447746cb72fefac2d6d90ee3143
a915ac4688028805905a68eb8f8a96674b093c495eddd8704461eaa2b345efbb2ad6930acd8023f870":MBEDTLS_RS
A_PKCS_V15:MBEDTLS_MD_SHA256:2048:16:"e79a373182bfaa722eb035f772ad2a9464bd842de59432c18bba
b3a7dfeae318c9b915ee487861ab665a40bd6cda560152578e8579016c929df99fea05b4d64efca1d543850bc8164b40d
71ed7f3fa4105df0fb9b9ad2a18ce182c8a4f4f975bea9aa0b9a1438a27a28e97ac8330ef37383414d1bd64607d6979ac0
50424fd17":16:"c6749cbb0db8c5a177672d4728a8b22392b2fc4d3b8361d5c0d5055a1b4e46d821f757c24eef2a51c5
61941b93b3ace7340074c058c9bb48e7e7414f42c41da4cccb5c2ba91deb30c586b7fb18af12a52995592ad139d3be42
9add6547e044becedaf31fa3b39421e24ee034fbf367d11f6b8f88ee483d163b431e1654ad3e89":16:"b38ac65c8141f7f
5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46
b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c
3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24
190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab535
1f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0
961a7b4c1a2034f":16:"3":"5aee2b9dbc02a6a2d87ff64a64165dc0b9ce70c79bab2d287939e2601c3223e0493988d54
68731ae4edc7d5f5d449335c204fdb0e192c1915c9d694d3a61c3be14df79c4b34d6ac73707829024d263c94f9107fa93

f3783de3965522336e18d1e01a142b5103451bb97839eaf2f44703a63050a36b78aef4072ea1a8daaaf1a2918fc03ee95
7a9c09efdc7287bcb4d6aec4723290294b249b3e3dc63157b560ad9c867323a73ebeb360cc9e482111643b0d86c4e33d
cf170155590f0eba7d170789e84de336b7fe2f6cf485ddca94607a4ff379fc49d375c730249dd1a210e7dccd762d1c23c7
532e769c6aa88e38e8654ff90f7b34df4c07ba90e89099ec1ed":0

RSA
PKCS1 Sign #2 Verify
depends_on:MBEDTLS_SHA256_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"59779fd2a39e56640c4fc1e67b60aeffcecd78aed7ad2bdfa464e93d04198d48466b8da744
5f25bfa19db2844edd5c8f539cf772cc132b483169d390db28a43bc4ee0f038f6568ffc87447746cb72fefac2d6d90ee31
43a915ac4688028805905a68eb8f8a96674b093c495eddd8704461eaa2b345efbb2ad6930acd8023f870":MBEDTLS_
RSA_PKCS_V15:MBEDTLS_MD_SHA256:2048:16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac1
2c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e4
6668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255ad
b0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf
93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e1
6d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"3":"5aee2b9dbc02a6
a2d87ff64a64165dc0b9ce70c79bab2d287939e2601c3223e0493988d5468731ae4edc7d5f5d449335c204fdb0e192c1
915c9d694d3a61c3be14df79c4b34d6ac73707829024d263c94f9107fa93f3783de3965522336e18d1e01a142b510345
1bb97839eaf2f44703a63050a36b78aef4072ea1a8daaaf1a2918fc03ee957a9c09efdc7287bcb4d6aec4723290294b249
b3e3dc63157b560ad9c867323a73ebeb360cc9e482111643b0d86c4e33dcf170155590f0eba7d170789e84de336b7fe2
f6cf485ddca94607a4ff379fc49d375c730249dd1a210e7dccd762d1c23c7532e769c6aa88e38e8654ff90f7b34df4c07b
a90e89099ec1ed":0

RSA
PKCS1 Sign #2 Verify (Fail)
depends_on:MBEDTLS_SHA256_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"59779fd2a39e56640c4fc1e67b60aeffcecd78aed7ad2bdfa464e93d04198d48466b8da744
5f25bfa19db2844edd5c8f539cf772cc132b483169d390db28a43bc4ee0f038f6568ffc87447746cb72fefac2d6d90ee31
43a915ac4688028805905a68eb8f8a96674b093c495eddd8704461eaa2b345efbb2ad6930acd8023f870":MBEDTLS_
RSA_PKCS_V15:MBEDTLS_MD_SHA256:2048:16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac1
2c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e4
6668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255ad
b0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf
93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e1
6d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"3":"5aee2b9dbc02a6
a2d87ff64a64165dc0b9ce70c79bab2d287939e2601c3223e0493988d5468731ae4edc7d5f5d449335c204fdb0e192c1
915c9d694d3a61c3be14df79c4b34d6ac73707829024d263c94f9107fa93f3783de3965522336e18d1e01a142b510345
1bb97839eaf2f44703a63050a36b78aef4072ea1a8daaaf1a2918fc03ee957a9c09efdc6287bcb4d6aec4723290294b249
b3e3dc63157b560ad9c867323a73ebeb360cc9e482111643b0d86c4e33dcf170155590f0eba7d170789e84de336b7fe2
f6cf485ddca94607a4ff379fc49d375c730249dd1a210e7dccd763d1c23c7532e769c6aa88e38e8654ff90f7b34df4c07b
a90e89099ec1ed":MBEDTLS_ERR_RSA_INVALID_PADDING

RSA
PKCS1 Sign #3 (SHA224, 2048 bits RSA)
depends_on:MBEDTLS_SHA256_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_sign:"59779fd2a39e56640c4fc1e67b60aeffcecd78aed7ad2bdfa464e93d04198d48466b8da7445f
25bfa19db2844edd5c8f539cf772cc132b483169d390db28a43bc4ee0f038f6568ffc87447746cb72fefac2d6d90ee3143

a915ac4688028805905a68eb8f8a96674b093c495eddd8704461eaa2b345efbb2ad6930acd8023f870":MBEDTLS_RS
A_PKCS_V15:MBEDTLS_MD_SHA224:2048:16:"e79a373182bfaa722eb035f772ad2a9464bd842de59432c18bba
b3a7dfeae318c9b915ee487861ab665a40bd6cda560152578e8579016c929df99fea05b4d64efca1d543850bc8164b40d
71ed7f3fa4105df0fb9b9ad2a18ce182c8a4f4f975bea9aa0b9a1438a27a28e97ac8330ef37383414d1bd64607d6979ac0
50424fd17":16:"c6749cbb0db8c5a177672d4728a8b22392b2fc4d3b8361d5c0d5055a1b4e46d821f757c24eef2a51c5
61941b93b3ace7340074c058c9bb48e7e7414f42c41da4cccb5c2ba91deb30c586b7fb18af12a52995592ad139d3be42
9add6547e044becedaf31fa3b39421e24ee034fbf367d11f6b8f88ee483d163b431e1654ad3e89":16:"b38ac65c8141f7f
5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46
b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c
3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24
190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab535
1f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0
961a7b4c1a2034f":16:"3":"9d768b8b31421f9d9ced890aafaf8b3468656419049ed268f6e1992066f45dc3e4cd349e8c
5ed5a06e4ef5badaba064ba94907dfedf3d708becaf44ae9b27c3866d329311ba93e8ddc7fc284fba05d1bb84fb1e060a5
b76b7fa515cfcd2c8144474623672703cac1e15ff4fdf8ef19d365c51ba86e60f4cbbcd07f956060625751bfbecc479456
46459cadaddd900603a8149a93b31a6d432e1da1a67eb765f5b2f0bd1adb9af12d731c7b02931b42dbbfd8c7cecde76b
817e96f664147a2c5091c6ce4dc562c5f57159d6f9dc9ba2daa212db56677839621bd4805dde62955fb2d0cc2c448109
d10ecc6206ea81f0a02e1646471358f3ec146cd3c75f2d390b":0

RSA
PKCS1 Sign #3 Verify
depends_on:MBEDTLS_SHA256_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"59779fd2a39e56640c4fc1e67b60aeffcecd78aed7ad2bdfa464e93d04198d48466b8da744
5f25bfa19db2844edd5c8f539cf772cc132b483169d390db28a43bc4ee0f038f6568ffc87447746cb72fefac2d6d90ee31
43a915ac4688028805905a68eb8f8a96674b093c495eddd8704461eaa2b345efbb2ad6930acd8023f870":MBEDTLS_
RSA_PKCS_V15:MBEDTLS_MD_SHA224:2048:16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac1
2c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e4
6668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255ad
b0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf
93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e1
6d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"3":"9d768b8b31421
f9d9ced890aafaf8b3468656419049ed268f6e1992066f45dc3e4cd349e8c5ed5a06e4ef5badaba064ba94907dfedf3d70
8becaf44ae9b27c3866d329311ba93e8ddc7fc284fba05d1bb84fb1e060a5b76b7fa515cfcd2c8144474623672703cac1
e15ff4fdf8ef19d365c51ba86e60f4cbbcd07f956060625751bfbecc47945646459cadaddd900603a8149a93b31a6d432e
1da1a67eb765f5b2f0bd1adb9af12d731c7b02931b42dbbfd8c7cecde76b817e96f664147a2c5091c6ce4dc562c5f5715
9d6f9dc9ba2daa212db56677839621bd4805dde62955fb2d0cc2c448109d10ecc6206ea81f0a02e1646471358f3ec146
cd3c75f2d390b":0

RSA
PKCS1 Sign #4 (SHA384, 2048 bits RSA)
depends_on:MBEDTLS_SHA512_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_sign:"59779fd2a39e56640c4fc1e67b60aeffcecd78aed7ad2bdfa464e93d04198d48466b8da7445f
25bfa19db2844edd5c8f539cf772cc132b483169d390db28a43bc4ee0f038f6568ffc87447746cb72fefac2d6d90ee3143
a915ac4688028805905a68eb8f8a96674b093c495eddd8704461eaa2b345efbb2ad6930acd8023f870":MBEDTLS_RS
A_PKCS_V15:MBEDTLS_MD_SHA384:2048:16:"e79a373182bfaa722eb035f772ad2a9464bd842de59432c18bba
b3a7dfeae318c9b915ee487861ab665a40bd6cda560152578e8579016c929df99fea05b4d64efca1d543850bc8164b40d
71ed7f3fa4105df0fb9b9ad2a18ce182c8a4f4f975bea9aa0b9a1438a27a28e97ac8330ef37383414d1bd64607d6979ac0
50424fd17":16:"c6749cbb0db8c5a177672d4728a8b22392b2fc4d3b8361d5c0d5055a1b4e46d821f757c24eef2a51c5

61941b93b3ace7340074c058c9bb48e7e7414f42c41da4cccb5c2ba91deb30c586b7fb18af12a52995592ad139d3be42
9add6547e044becedaf31fa3b39421e24ee034fbf367d11f6b8f88ee483d163b431e1654ad3e89":16:"b38ac65c8141f7f
5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46
b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c
3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24
190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab535
1f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0
961a7b4c1a2034f":16:"3":"40dcc96822e5612eb33f1dca247a35109ba3845c7a3d556a60e656624bf1c103d94686ca7
379e9e329ccd1b19b52bfd48b608df9f59a96a82d3feb0101096dbcb80e46da543b4c982ac6bb1717f24f9fe3f76b7154
492b47525be1ddcaf4631d33481531be8f3e685837b40bdf4a02827d79f6a32374147174680f51c8e0d8eed9d5c445a5
63a7bce9ef4236e7cfdc12b2223ef457c3e8ccc6dd65cc23e977a1f03f5ef584feb9af00efc71a701f9d413b0290af17692c
b821a1e863d5778e174b1130659f30583f434f09cb1212471a41dd65c102de64a194b6ae3e43cd75928049db78042c58
e980aff3ea2774e42845bcf217410a118cf5deeaa64224dbc8":0

RSA
PKCS1 Sign #4 Verify
depends_on:MBEDTLS_SHA512_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"59779fd2a39e56640c4fc1e67b60aeffcecd78aed7ad2bdfa464e93d04198d48466b8da744
5f25bfa19db2844edd5c8f539cf772cc132b483169d390db28a43bc4ee0f038f6568ffc87447746cb72fefac2d6d90ee31
43a915ac4688028805905a68eb8f8a96674b093c495eddd8704461eaa2b345efbb2ad6930acd8023f870":MBEDTLS_
RSA_PKCS_V15:MBEDTLS_MD_SHA384:2048:16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac1
2c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e4
6668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255ad
b0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf
93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e1
6d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"3":"40dcc96822e56
12eb33f1dca247a35109ba3845c7a3d556a60e656624bf1c103d94686ca7379e9e329ccd1b19b52bfd48b608df9f59a96
a82d3feb0101096dbcb80e46da543b4c982ac6bb1717f24f9fe3f76b7154492b47525be1ddcaf4631d33481531be8f3e6
85837b40bdf4a02827d79f6a32374147174680f51c8e0d8eed9d5c445a563a7bce9ef4236e7cfdc12b2223ef457c3e8cc
c6dd65cc23e977a1f03f5ef584feb9af00efc71a701f9d413b0290af17692cb821a1e863d5778e174b1130659f30583f43
4f09cb1212471a41dd65c102de64a194b6ae3e43cd75928049db78042c58e980aff3ea2774e42845bcf217410a118cf5d
eeaa64224dbc8":0

RSA
PKCS1 Sign #5 (MD2, 2048 bits RSA)
depends_on:MBEDTLS_MD2_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_sign:"59779fd2a39e56640c4fc1e67b60aeffcecd78aed7ad2bdfa464e93d04198d48466b8da7445f
25bfa19db2844edd5c8f539cf772cc132b483169d390db28a43bc4ee0f038f6568ffc87447746cb72fefac2d6d90ee3143
a915ac4688028805905a68eb8f8a96674b093c495eddd8704461eaa2b345efbb2ad6930acd8023f870":MBEDTLS_RS
A_PKCS_V15:MBEDTLS_MD_MD2:2048:16:"e79a373182bfaa722eb035f772ad2a9464bd842de59432c18bbab3a
7dfeae318c9b915ee487861ab665a40bd6cda560152578e8579016c929df99fea05b4d64efca1d543850bc8164b40d71e
d7f3fa4105df0fb9b9ad2a18ce182c8a4f4f975bea9aa0b9a1438a27a28e97ac8330ef37383414d1bd64607d6979ac0504
24fd17":16:"c6749cbb0db8c5a177672d4728a8b22392b2fc4d3b8361d5c0d5055a1b4e46d821f757c24eef2a51c5619
41b93b3ace7340074c058c9bb48e7e7414f42c41da4cccb5c2ba91deb30c586b7fb18af12a52995592ad139d3be429ad
d6547e044becedaf31fa3b39421e24ee034fbf367d11f6b8f88ee483d163b431e1654ad3e89":16:"b38ac65c8141f7f5c9
6e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94
813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee
0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b2419

0965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"3":"6cbb0e4019d64dd5cd2d48fa43446e5cba1a7edbb79d91b199be75c7d3e7ae0820c44d3a120cd2910f73cbb315e15963a60ea7da3452015d9d6beb5ac998fddbd1fa3e5908abc9151f3ffb70365aaee6fb0cd440d3f5591868fc136fae38ac7bcdb3bde3c6a0362dd8b814f7edadd4a51b2edf2227a40d1e34c29f608add7746731425858eb93661c633b7a90942fca3cd594ab4ec170052d44105643518020782e76235def34d014135bad8daed590200482325c3416c3d66417e80d9f9c6322a54683638247b577445ecd0be2765ce96c4ee45213204026dfba24d5ee89e1ea75538ba39f7149a5ac0fc12d7c53cbc12481d4a8e2d410ec633d800ad4b4304":0

RSA
PKCS1 Sign #5 Verify
depends_on:MBEDTLS_MD2_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"59779fd2a39e56640c4fc1e67b60aeffcecd78aed7ad2bdfa464e93d04198d48466b8da7445f25bfa19db2844edd5c8f539cf772cc132b483169d390db28a43bc4ee0f038f6568ffc87447746cb72fefac2d6d90ee3143a915ac4688028805905a68eb8f8a96674b093c495eddd8704461eaa2b345efbb2ad6930acd8023f870":MBEDTLS_RSA_PKCS_V15:MBEDTLS_MD_MD2:2048:16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"3":"6cbb0e4019d64dd5cd2d48fa43446e5cba1a7edbb79d91b199be75c7d3e7ae0820c44d3a120cd2910f73cbb315e15963a60ea7da3452015d9d6beb5ac998fddbd1fa3e5908abc9151f3ffb70365aaee6fb0cd440d3f5591868fc136fae38ac7bcdb3bde3c6a0362dd8b814f7edadd4a51b2edf2227a40d1e34c29f608add7746731425858eb93661c633b7a90942fca3cd594ab4ec170052d44105643518020782e76235def34d014135bad8daed590200482325c3416c3d66417e80d9f9c6322a54683638247b577445ecd0be2765ce96c4ee45213204026dfba24d5ee89e1ea75538ba39f7149a5ac0fc12d7c53cbc12481d4a8e2d410ec633d800ad4b4304":0

RSA
PKCS1 Sign #6 (MD4, 2048 bits RSA)
depends_on:MBEDTLS_MD4_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_sign:"59779fd2a39e56640c4fc1e67b60aeffcecd78aed7ad2bdfa464e93d04198d48466b8da7445f25bfa19db2844edd5c8f539cf772cc132b483169d390db28a43bc4ee0f038f6568ffc87447746cb72fefac2d6d90ee3143a915ac4688028805905a68eb8f8a96674b093c495eddd8704461eaa2b345efbb2ad6930acd8023f870":MBEDTLS_RSA_PKCS_V15:MBEDTLS_MD_MD4:2048:16:"e79a373182bfaa722eb035f772ad2a9464bd842de59432c18bbab3a7dfeae318c9b915ee487861ab665a40bd6cda560152578e8579016c929df99fea05b4d64efca1d543850bc8164b40d71ed7f3fa4105df0fb9b9ad2a18ce182c8a4f4f975bea9aa0b9a1438a27a28e97ac8330ef37383414d1bd64607d6979ac050424fd17":16:"c6749cbb0db8c5a177672d4728a8b22392b2fc4d3b8361d5c0d5055a1b4e46d821f757c24eef2a51c561941b93b3ace7340074c058c9bb48e7e7414f42c41da4cccb5c2ba91deb30c586b7fb18af12a52995592ad139d3be429add6547e044becedaf31fa3b39421e24ee034fbf367d11f6b8f88ee483d163b431e1654ad3e89":16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b240190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"3":"b0e60dc4dfaf0f636a3a4414eae2d7bce7c3ce505a46e38f3f654d8769b31b7891ba18f89672fce204bbac6e3764355e65447c087994731cd44f086710e79e8c3ebc6e2cb61edc5d3e05848ab733d95efe2d0252a691e810c17fa57fd2dd296374c9ba17fea704685677f45d668a386c8ca433fbbb56d3bbfb43a489ed9518b1c9ab13ce497a1c

ec91467453bfe533145a31a095c2de541255141768ccc6fdff3fc790b5050f1122c93c3044a9346947e1b23e8125bf7ed
bf38c64a4286dfc1b829e983db3117959a2559a8ef97687ab673e231be213d88edc632637b58cdb2d69c51fbf6bf894cf
f319216718b1e696f75cd4366f53dc2e28b2a00017984207":0

RSA
PKCS1 Sign #6 Verify
depends_on:MBEDTLS_MD4_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"59779fd2a39e56640c4fc1e67b60aeffcecd78aed7ad2bdfa464e93d04198d48466b8da744
5f25bfa19db2844edd5c8f539cf772cc132b483169d390db28a43bc4ee0f038f6568ffc87447746cb72fefac2d6d90ee31
43a915ac4688028805905a68eb8f8a96674b093c495eddd8704461eaa2b345efbb2ad6930acd8023f870":MBEDTLS_
RSA_PKCS_V15:MBEDTLS_MD_MD4:2048:16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c
05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e466
68ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0
add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93
c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d
064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"3":"b0e60dc4dfaf0f63
6a3a4414eae2d7bce7c3ce505a46e38f3f654d8769b31b7891ba18f89672fce204bbac6e3764355e65447c087994731cd
44f086710e79e8c3ebc6e2cb61edc5d3e05848ab733d95efe2d0252a691e810c17fa57fd2dd296374c9ba17fea7046856
77f45d668a386c8ca433fbbb56d3bbfb43a489ed9518b1c9ab13ce497a1cec91467453bfe533145a31a095c2de5412551
41768ccc6fdff3fc790b5050f1122c93c3044a9346947e1b23e8125bf7edbf38c64a4286dfc1b829e983db3117959a255
9a8ef97687ab673e231be213d88edc632637b58cdb2d69c51fbf6bf894cff319216718b1e696f75cd4366f53dc2e28b2a
00017984207":0

RSA
PKCS1 Sign #7 (MD5, 2048 bits RSA)
depends_on:MBEDTLS_MD5_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_sign:"59779fd2a39e56640c4fc1e67b60aeffcecd78aed7ad2bdfa464e93d04198d48466b8da7445f
25bfa19db2844edd5c8f539cf772cc132b483169d390db28a43bc4ee0f038f6568ffc87447746cb72fefac2d6d90ee3143
a915ac4688028805905a68eb8f8a96674b093c495eddd8704461eaa2b345efbb2ad6930acd8023f870":MBEDTLS_RS
A_PKCS_V15:MBEDTLS_MD_MD5:2048:16:"e79a373182bfaa722eb035f772ad2a9464bd842de59432c18bbab3a
7dfeae318c9b915ee487861ab665a40bd6cda560152578e8579016c929df99fea05b4d64efca1d543850bc8164b40d71e
d7f3fa4105df0fb9b9ad2a18ce182c8a4f4f975bea9aa0b9a1438a27a28e97ac8330ef37383414d1bd64607d6979ac0504
24fd17":16:"c6749cbb0db8c5a177672d4728a8b22392b2fc4d3b8361d5c0d5055a1b4e46d821f757c24eef2a51c5619
41b93b3ace7340074c058c9bb48e7e7414f42c41da4cccb5c2ba91deb30c586b7fb18af12a52995592ad139d3be429ad
d6547e044becedaf31fa3b39421e24ee034fbf367d11f6b8f88ee483d163b431e1654ad3e89":16:"b38ac65c8141f7f5c9
6e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94
813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee
0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b2419
0965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f9
7a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b096
1a7b4c1a2034f":16:"3":"3bcf673c3b27f6e2ece4bb97c7a37161e6c6ee7419ef366efc3cfee0f15f415ff6d9d439093738
6c6fec1771acba73f24ec6b0469ea8b88083f0b4e1b6069d7bf286e67cf94182a548663137e82a6e09c35de2c27779da0
503f1f5bedfebadf2a875f17763a0564df4a6d945a5a3e46bc90fb692af3a55106aafc6b577587456ff8d49cfd5c299d7a2
b776dbe4c1ae777b0f64aa3bab27689af32d6cc76157c7dc6900a3469e18a7d9b6bfe4951d1105a08864575e4f4ec05b3
e053f9b7a2d5653ae085e50a63380d6bdd6f58ab378d7e0a2be708c5598498913170 89ab04c82d8bc589ea088b90b11d
ea5cf85856ff7e609cc1adb1d403beead4c126ff29021":0

RSA

PKCS1 Sign #7 Verify
depends_on:MBEDTLS_MD5_C:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"59779fd2a39e56640c4fc1e67b60aeffcecd78aed7ad2bdfa464e93d04198d48466b8da7445f25bfa19db2844edd5c8f539cf772cc132b483169d390db28a43bc4ee0f038f6568ffc87447746cb72fefac2d6d90ee3143a915ac4688028805905a68eb8f8a96674b093c495eddd8704461eaa2b345efbb2ad6930acd8023f870":MBEDTLS_RSA_PKCS_V15:MBEDTLS_MD_MD5:2048:16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"3":"3bcf673c3b27f6e2ece4bb97c7a37161e6c6ee7419ef366efc3cfee0f15f415ff6d9d4390937386c6fec1771acba73f24ec6b0469ea8b88083f0b4e1b6069d7bf286e67cf94182a548663137e82a6e09c35de2c27779da0503f1f5bedfebadf2a875f17763a0564df4a6d945a5a3e46bc90fb692af3a55106aafc6b577587456ff8d49cfd5c299d7a2b776dbe4c1ae777b0f64aa3bab27689af32d6cc76157c7dc6900a3469e18a7d9b6bfe4951d1105a08864575e4f4ec05b3e053f9b7a2d5653ae085e50a63380d6bdd6f58ab378d7e0a2be708c559849891317089ab04c82d8bc589ea088b90b11dea5cf85856ff7e609cc1adb1d403beead4c126ff29021":0

RSA
PKCS1 Sign #8 (RAW, 2048 bits RSA)
depends_on:MBEDTLS_PKCS1_V15
rsa_pkcs1_sign_raw:"59779fd2a39e56640c4fc1e67b60aeffcecd78aed7ad2bdfa464e93d04198d48466b8da7445f25bfa19db2844edd5c8f539cf772cc132b483169d390db28a43bc4ee0f038f6568ffc87447746cb72fefac2d6d90ee3143a915ac4688028805905a68eb8f8a96674b093c495eddd8704461eaa2b345efbb2ad6930acd8023f870":"1234567890deadbeef":MBEDTLS_RSA_PKCS_V15:2048:16:"e79a373182bfaa722eb035f772ad2a9464bd842de59432c18bbab3a7dfeae318c9b915ee487861ab665a40bd6cda560152578e8579016c929df99fea05b4d64efca1d543850bc8164b40d71ed7f3fa4105df0fb9b9ad2a18ce182c8a4f4f975bea9aa0b9a1438a27a28e97ac8330ef37383414d1bd64607d6979ac050424fd17":16:"c6749cbb0db8c5a177672d4728a8b22392b2fc4d3b8361d5c0d5055a1b4e46d821f757c24eef2a51c561941b93b3ace7340074c058c9bb48e7e7414f42c41da4cccb5c2ba91deb30c586b7fb18af12a52995592ad139d3be429add6547e044becedaf31fa3b39421e24ee034fbf367d11f6b8f88ee483d163b431e1654ad3e89":16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"3":"605baf947c0de49e4f6a0dfb94a43ae318d5df8ed20ba4ba5a37a73fb009c5c9e5cce8b70a25b1c7580f389f0d7092485cdfa02208b70d33482edf07a7eafebdc54862ca0e0396a5a7d09991b9753eb1ffb6091971bb5789c6b121abbcd0a3cbaa39969fa7c28146fce96c6d03272e3793e5be8f5abfa9afcbebb986d7b3050604a2af4d3a40fa6c003781a539a60259d1e84f13322da9e538a49c369b83e7286bf7d30b64bbb773506705da5d5d5483a563a1ffacc902fb75c9a751b1e83cdc7a6db0470056883f48b5a5446b43b1d180ea12ba11a6a8d93b3b32a30156b6084b7fb142998a2a0d28014b84098ece7d9d5e4d55cc342ca26f5a0167a679dec8"

RSA
PKCS1 Sign #8 Verify
depends_on:MBEDTLS_PKCS1_V15
rsa_pkcs1_verify_raw:"59779fd2a39e56640c4fc1e67b60aeffcecd78aed7ad2bdfa464e93d04198d48466b8da7445f25bfa19db2844edd5c8f539cf772cc132b483169d390db28a43bc4ee0f038f6568ffc87447746cb72fefac2d6d90ee3143a915ac4688028805905a68eb8f8a96674b093c495eddd8704461eaa2b345efbb2ad6930acd8023f870":"1234567890dead

beef":MBEDTLS_RSA_PKCS_V15:2048:16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c
0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ac
e68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add
2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b
8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064
d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"3":"605baf947c0de49e4f6
a0dfb94a43ae318d5df8ed20ba4ba5a37a73fb009c5c9e5cce8b70a25b1c7580f389f0d7092485cdfa02208b70d33482e
df07a7eafebdc54862ca0e0396a5a7d09991b9753eb1ffb6091971bb5789c6b121abbcd0a3cbaa39969fa7c28146fce96c
6d03272e3793e5be8f5abfa9afcbebb986d7b3050604a2af4d3a40fa6c003781a539a60259d1e84f13322da9e538a49c3
69b83e7286bf7d30b64bbb773506705da5d5d5483a563a1ffacc902fb75c9a751b1e83cdc7a6db0470056883f48b5a54
46b43b1d180ea12ba11a6a8d93b3b32a30156b6084b7fb142998a2a0d28014b84098ece7d9d5e4d55cc342ca26f5a016
7a679dec8":0

RSA
PKCS1 Sign #8 Verify (Wrong raw hash)
depends_on:MBEDTLS_PKCS1_V15
rsa_pkcs1_verify_raw:"59779fd2a39e56640c4fc1e67b60aeffcecd78aed7ad2bdfa464e93d04198d48466b8da7445f25
bfa19db2844edd5c8f539cf772cc132b483169d390db28a43bc4ee0f038f6568ffc87447746cb72fefac2d6d90ee3143a9
15ac4688028805905a68eb8f8a96674b093c495eddd8704461eaa2b345efbb2ad6930acd8023f870":"1234567890dead
cafe":MBEDTLS_RSA_PKCS_V15:2048:16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c
0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ac
e68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add
2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b
8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064
d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"3":"605baf947c0de49e4f6
a0dfb94a43ae318d5df8ed20ba4ba5a37a73fb009c5c9e5cce8b70a25b1c7580f389f0d7092485cdfa02208b70d33482e
df07a7eafebdc54862ca0e0396a5a7d09991b9753eb1ffb6091971bb5789c6b121abbcd0a3cbaa39969fa7c28146fce96c
6d03272e3793e5be8f5abfa9afcbebb986d7b3050604a2af4d3a40fa6c003781a539a60259d1e84f13322da9e538a49c3
69b83e7286bf7d30b64bbb773506705da5d5d5483a563a1ffacc902fb75c9a751b1e83cdc7a6db0470056883f48b5a54
46b43b1d180ea12ba11a6a8d93b3b32a30156b6084b7fb142998a2a0d28014b84098ece7d9d5e4d55cc342ca26f5a016
7a679dec8":MBEDTLS_ERR_RSA_VERIFY_FAILED

RSA
PKCS1 Sign #9 (Invalid Digest type)
depends_on:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_sign:"59779fd2a39e56640c4fc1e67b60aeffcecd78aed7ad2bdfa464e93d04198d48466b8da7445f
25bfa19db2844edd5c8f539cf772cc132b483169d390db28a43bc4ee0f038f6568ffc87447746cb72fefac2d6d90ee3143
a915ac4688028805905a68eb8f8a96674b093c495eddd8704461eaa2b345efbb2ad6930acd8023f870":MBEDTLS_RS
A_PKCS_V15:255:2048:16:"e79a373182bfaa722eb035f772ad2a9464bd842de59432c18bbab3a7dfeae318c9b915ee
487861ab665a40bd6cda560152578e8579016c929df99fea05b4d64efca1d543850bc8164b40d71ed7f3fa4105df0fb9b
9ad2a18ce182c8a4f4f975bea9aa0b9a1438a27a28e97ac8330ef37383414d1bd64607d6979ac050424fd17":16:"c6749
cbb0db8c5a177672d4728a8b22392b2fc4d3b8361d5c0d5055a1b4e46d821f757c24eef2a51c561941b93b3ace734007
4c058c9bb48e7e7414f42c41da4cccb5c2ba91deb30c586b7fb18af12a52995592ad139d3be429add6547e044becedaf3
1fa3b39421e24ee034fbf367d11f6b8f88ee483d163b431e1654ad3e89":16:"b38ac65c8141f7f5c96e14470e851936a6
7bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c
482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c98
26e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35
255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b145

8b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"
3":"3bcf673c3b27f6e2ece4bb97c7a37161e6c6ee7419ef366efc3cfee0f15f415ff6d9d4390937386c6fec1771acba73f2
4ec6b0469ea8b88083f0b4e1b6069d7bf286e67cf94182a548663137e82a6e09c35de2c27779da0503f1f5bedfebadf2a8
75f17763a0564df4a6d945a5a3e46bc90fb692af3a55106aafc6b577587456ff8d49cfd5c299d7a2b776dbe4c1ae777b0f
64aa3bab27689af32d6cc76157c7dc6900a3469e18a7d9b6bfe4951d1105a08864575e4f4ec05b3e053f9b7a2d5653ae0
85e50a63380d6bdd6f58ab378d7e0a2be708c559849891317089ab04c82d8bc589ea088b90b11dea5cf85856ff7e609c
c1adb1d403beead4c126ff29021":MBEDTLS_ERR_RSA_BAD_INPUT_DATA

RSA
PKCS1 Sign #9 Verify (Invalid Digest type)
depends_on:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_verify:"59779fd2a39e56640c4fc1e67b60aeffcecd78aed7ad2bdfa464e93d04198d48466b8da744
5f25bfa19db2844edd5c8f539cf772cc132b483169d390db28a43bc4ee0f038f6568ffc87447746cb72fefac2d6d90ee31
43a915ac4688028805905a68eb8f8a96674b093c495eddd8704461eaa2b345efbb2ad6930acd8023f870":MBEDTLS_
RSA_PKCS_V15:255:2048:16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba
2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6
681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1
b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448
de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c238
93d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"3":"3bcf673c3b27f6e2ece4bb97c7a37161
e6c6ee7419ef366efc3cfee0f15f415ff6d9d4390937386c6fec1771acba73f24ec6b0469ea8b88083f0b4e1b6069d7bf28
6e67cf94182a548663137e82a6e09c35de2c27779da0503f1f5bedfebadf2a875f17763a0564df4a6d945a5a3e46bc90fb
692af3a55106aafc6b577587456ff8d49cfd5c299d7a2b776dbe4c1ae777b0f64aa3bab27689af32d6cc76157c7dc6900a
3469e18a7d9b6bfe4951d1105a08864575e4f4ec05b3e053f9b7a2d5653ae085e50a63380d6bdd6f58ab378d7e0a2be7
08c559849891317089ab04c82d8bc589ea088b90b11dea5cf85856ff7e609cc1adb1d403beead4c126ff29021":MBED
TLS_ERR_RSA_BAD_INPUT_DATA

RSA
PKCS1 Sign #8 (Invalid padding type)
mbedtls_rsa_pkcs1_sign:"59779fd2a39e56640c4fc1e67b60aeffcecd78aed7ad2bdfa464e93d04198d48466b8da7445f
25bfa19db2844edd5c8f539cf772cc132b483169d390db28a43bc4ee0f038f6568ffc87447746cb72fefac2d6d90ee3143
a915ac4688028805905a68eb8f8a96674b093c495eddd8704461eaa2b345efbb2ad6930acd8023f870":2:MBEDTLS_
MD_MD5:2048:16:"e79a373182bfaa722eb035f772ad2a9464bd842de59432c18bbab3a7dfeae318c9b915ee487861a
b665a40bd6cda560152578e8579016c929df99fea05b4d64efca1d543850bc8164b40d71ed7f3fa4105df0fb9b9ad2a18
ce182c8a4f4f975bea9aa0b9a1438a27a28e97ac8330ef37383414d1bd64607d6979ac050424fd17":16:"c6749cbb0db8
c5a177672d4728a8b22392b2fc4d3b8361d5c0d5055a1b4e46d821f757c24eef2a51c561941b93b3ace7340074c058c9
bb48e7e7414f42c41da4cccb5c2ba91deb30c586b7fb18af12a52995592ad139d3be429add6547e044becedaf31fa3b39
421e24ee034fbf367d11f6b8f88ee483d163b431e1654ad3e89":16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6
821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830
bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673b
f8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b352557652
61cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97dae
d4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"3":"3bcf
673c3b27f6e2ece4bb97c7a37161e6c6ee7419ef366efc3cfee0f15f415ff6d9d4390937386c6fec1771acba73f24ec6b04
69ea8b88083f0b4e1b6069d7bf286e67cf94182a548663137e82a6e09c35de2c27779da0503f1f5bedfebadf2a875f1776
3a0564df4a6d945a5a3e46bc90fb692af3a55106aafc6b577587456ff8d49cfd5c299d7a2b776dbe4c1ae777b0f64aa3ba
b27689af32d6cc76157c7dc6900a3469e18a7d9b6bfe4951d1105a08864575e4f4ec05b3e053f9b7a2d5653ae085e50a6
3380d6bdd6f58ab378d7e0a2be708c559849891317089ab04c82d8bc589ea088b90b11dea5cf85856ff7e609cc1adb1d

403beead4c126ff29021":MBEDTLS_ERR_RSA_INVALID_PADDING

RSA
PKCS1 Sign #8 Verify (Invalid padding type)
mbedtls_rsa_pkcs1_verify:"59779fd2a39e56640c4fc1e67b60aeffcecd78aed7ad2bdfa464e93d04198d48466b8da744
5f25bfa19db2844edd5c8f539cf772cc132b483169d390db28a43bc4ee0f038f6568ffc87447746cb72fefac2d6d90ee31
43a915ac4688028805905a68eb8f8a96674b093c495eddd8704461eaa2b345efbb2ad6930acd8023f870":1:MBEDTLS
_MD_MD5:2048:16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b
02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf
1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe
6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b
813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222
793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"3":"3bcf673c3b27f6e2ece4bb97c7a37161e6c6ee7419
ef366efc3cfee0f15f415ff6d9d4390937386c6fec1771acba73f24ec6b0469ea8b88083f0b4e1b6069d7bf286e67cf9418
2a548663137e82a6e09c35de2c27779da0503f1f5bedfebadf2a875f17763a0564df4a6d945a5a3e46bc90fb692af3a551
06aafc6b577587456ff8d49cfd5c299d7a2b776dbe4c1ae777b0f64aa3bab27689af32d6cc76157c7dc6900a3469e18a7
d9b6bfe4951d1105a08864575e4f4ec05b3e053f9b7a2d5653ae085e50a63380d6bdd6f58ab378d7e0a2be708c559849
891317089ab04c82d8bc589ea088b90b11dea5cf85856ff7e609cc1adb1d403beead4c126ff29021":MBEDTLS_ERR_
RSA_INVALID_PADDING

RSA
PKCS1 Encrypt #1
depends_on:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_encrypt:"4E636AF98E40F3ADCFCCB698F4E80B9F":MBEDTLS_RSA_PKCS_V15:2048:16
:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a84
17b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61
dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec5
9559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c22954
3d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f
35549141486c3b0961a7b4c1a2034f":16:"3":"b0c0b193ba4a5b4502bfacd1a9c2697da5510f3e3ab7274cf404418afd2
c62c89b98d83bbc21c8c1bf1afe6d8bf40425e053e9c03e03a3be0edbe1eda073fade1cc286cc0305a493d98fe795634c3
cad7feb513edb742d66d910c87d07f6b0055c3488bb262b5fd1ce8747af64801fb39d2d3a3e57086ffe55ab8d0a2ca869
75629a0f85767a4990c532a7c2dab1647997ebb234d0b28a0008bfebfc905e7ba5b30b60566a5e0190417465efdbf549
934b8f0c5c9f36b7c5b6373a47ae553ced0608a161b1b70dfa509375cf7a3598223a6d7b7a1d1a06ac74d345a9bb7c0e4
4c8388858a4f1d8115f2bd769ffa69020385fa286302c80e950f9e2751308666c":0

RSA
PKCS1 Decrypt #1 (Verify)
depends_on:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_decrypt:"a42eda41e56235e666e7faaa77100197f657288a1bf183e4820f0c37ce2c456b960278d6
003e0bbcd4be4a969f8e8fd9231e1f492414f00ed09844994c86ec32db7cde3bec7f0c3dbf6ae55baeb2712fa609f5fc32
07a824eb3dace31849cd6a6084318523912bccb84cf42e3c6d6d1685131d69bb545acec827d2b0dfdd5568b7dcc4f5a1
1d6916583fefa689d367f8c9e1d95dcd2240895a9470b0c1730f97cd6e8546860bd254801769f54be96e16362ddcbf34
d56035028890199e0f48db38642cb66a4181e028a6443a404fea284ce02b4614b683367d40874e505611d23142d49f0
6feea831d52d347b13610b413c4efc43a6de9f0b08d2a951dc503b6":MBEDTLS_RSA_PKCS_V15:2048:16:"e79a37
3182bfaa722eb035f772ad2a9464bd842de59432c18bbab3a7dfeae318c9b915ee487861ab665a40bd6cda560152578e
8579016c929df99fea05b4d64efca1d543850bc8164b40d71ed7f3fa4105df0fb9b9ad2a18ce182c8a4f4f975bea9aa0b9
a1438a27a28e97ac8330ef37383414d1bd64607d6979ac050424fd17":16:"c6749cbb0db8c5a177672d4728a8b22392b

2fc4d3b8361d5c0d5055a1b4e46d821f757c24eef2a51c561941b93b3ace7340074c058c9bb48e7e7414f42c41da4cccb
5c2ba91deb30c586b7fb18af12a52995592ad139d3be429add6547e044becedaf31fa3b39421e24ee034fbf367d11f6b8f
88ee483d163b431e1654ad3e89":16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6
ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace6890361
7faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a
7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cb
b448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8
c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"3":1000:"4E636AF98E40F3ADCFC
CB698F4E80B9F":0

RSA
PKCS1 Encrypt #2 (Data too large)
depends_on:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_encrypt:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba222
4703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681
f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4e
cf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4
715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d
755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":MBEDTLS_RSA_PKCS_V15:2048:16:"b38ac65
c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675
fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c
6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d
54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0
adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141
486c3b0961a7b4c1a2034f":16:"3":"a42eda41e56235e666e7faaa77100197f657288a1bf183e4820f0c37ce2c456b960
278d6003e0bbcd4be4a969f8e8fd9231e1f492414f00ed09844994c86ec32db7cde3bec7f0c3dbf6ae55baeb2712fa609f
5fc3207a824eb3dace31849cd6a6084318523912bccb84cf42e3c6d6d1685131d69bb545acec827d2b0dfdd5568b7dcc
4f5a11d6916583fefa689d367f8c9e1d95dcd2240895a9470b0c1730f97cd6e8546860bd254801769f54be96e16362ddc
bf34d56035028890199e0f48db38642cb66a4181e028a6443a404fea284ce02b4614b683367d40874e505611d23142d
49f06feea831d52d347b13610b413c4efc43a6de9f0b08d2a951dc503b6":MBEDTLS_ERR_RSA_BAD_INPUT_DA
TA

RSA
PKCS1 Decrypt
#2 (Data too small)
depends_on:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_decrypt:"deadbeafcafedeadbeeffedcba9876":MBEDTLS_RSA_PKCS_V15:2048:16:"e79a3731
82bfaa722eb035f772ad2a9464bd842de59432c18bbab3a7dfeae318c9b915ee487861ab665a40bd6cda560152578e85
79016c929df99fea05b4d64efca1d543850bc8164b40d71ed7f3fa4105df0fb9b9ad2a18ce182c8a4f4f975bea9aa0b9a1
438a27a28e97ac8330ef37383414d1bd64607d6979ac050424fd17":16:"c6749cbb0db8c5a177672d4728a8b22392b2f
c4d3b8361d5c0d5055a1b4e46d821f757c24eef2a51c561941b93b3ace7340074c058c9bb48e7e7414f42c41da4cccb5c
2ba91deb30c586b7fb18af12a52995592ad139d3be429add6547e044becedaf31fa3b39421e24ee034fbf367d11f6b8f88
ee483d163b431e1654ad3e89":16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6dd
ba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617fa
f6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bc
d1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb4
48de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c2
3893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"3":1000:"4E636AF98E40F3ADCFCCB

698F4E80B9F":MBEDTLS_ERR_RSA_PRIVATE_FAILED
+ MBEDTLS_ERR_MPI_BAD_INPUT_DATA

RSA PKCS1 Encrypt #3 (Invalid padding mode)
mbedtls_rsa_pkcs1_encrypt:"4E636AF98E40F3ADCFCCB698F4E80B9F":2:2048:16:"b38ac65c8141f7f5c96e1447
0e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7
b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc0790
8509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eaf
bdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810
c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c
1a2034f":16:"3":"a42eda41e56235e666e7faaa77100197f657288a1bf183e4820f0c37ce2c456b960278d6003e0bbcd4
be4a969f8e8fd9231e1f492414f00ed09844994c86ec32db7cde3bec7f0c3dbf6ae55baeb2712fa609f5fc3207a824eb3da
ce31849cd6a6084318523912bccb84cf42e3c6d6d1685131d69bb545acec827d2b0dfdd5568b7dcc4f5a11d6916583fef
a689d367f8c9e1d95dcd2240895a9470b0c1730f97cd6e8546860bd254801769f54be96e16362ddcbf34d56035028890
199e0f48db38642cb66a4181e028a6443a404fea284ce02b4614b683367d40874e505611d23142d49f06feea831d52d3
47b13610b413c4efc43a6de9f0b08d2a951dc503b6":MBEDTLS_ERR_RSA_INVALID_PADDING

RSA
PKCS1 Decrypt #3 (Invalid padding mode)
mbedtls_rsa_pkcs1_decrypt:"a42eda41e56235e666e7faaa77100197f657288a1bf183e4820f0c37ce2c456b960278d6
003e0bbcd4be4a969f8e8fd9231e1f492414f00ed09844994c86ec32db7cde3bec7f0c3dbf6ae55baeb2712fa609f5fc32
07a824eb3dace31849cd6a6084318523912bccb84cf42e3c6d6d1685131d69bb545acec827d2b0dfdd5568b7dcc4f5a1
1d6916583fefa689d367f8c9e1d95dcd2240895a9470b0c1730f97cd6e8546860bd254801769f54be96e16362ddcbf34
d56035028890199e0f48db38642cb66a4181e028a6443a404fea284ce02b4614b683367d40874e505611d23142d49f0
6feea831d52d347b13610b413c4efc43a6de9f0b08d2a951dc503b6":2:2048:16:"e79a373182bfaa722eb035f772ad2a9
464bd842de59432c18bbab3a7dfeae318c9b915ee487861ab665a40bd6cda560152578e8579016c929df99fea05b4d64
efca1d543850bc8164b40d71ed7f3fa4105df0fb9b9ad2a18ce182c8a4f4f975bea9aa0b9a1438a27a28e97ac8330ef373
83414d1bd64607d6979ac050424fd17":16:"c6749cbb0db8c5a177672d4728a8b22392b2fc4d3b8361d5c0d5055a1b4
e46d821f757c24eef2a51c561941b93b3ace7340074c058c9bb48e7e7414f42c41da4cccb5c2ba91deb30c586b7fb18af
12a52995592ad139d3be429add6547e044becedaf31fa3b39421e24ee034fbf367d11f6b8f88ee483d163b431e1654ad3
e89":16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452
f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420
d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da
486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c9482
9c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a7
8c3d64f35549141486c3b0961a7b4c1a2034f":16:"3":1000:"4E636AF98E40F3ADCFCCB698F4E80B9F":MBEDT
LS_ERR_RSA_INVALID_PADDING

RSA
PKCS1 Decrypt #4 (Output buffer too small)
depends_on:MBEDTLS_PKCS1_V15
mbedtls_rsa_pkcs1_decrypt:"a42eda41e56235e666e7faaa77100197f657288a1bf183e4820f0c37ce2c456b960278d6
003e0bbcd4be4a969f8e8fd9231e1f492414f00ed09844994c86ec32db7cde3bec7f0c3dbf6ae55baeb2712fa609f5fc32
07a824eb3dace31849cd6a6084318523912bccb84cf42e3c6d6d1685131d69bb545acec827d2b0dfdd5568b7dcc4f5a1
1d6916583fefa689d367f8c9e1d95dcd2240895a9470b0c1730f97cd6e8546860bd254801769f54be96e16362ddcbf34
d56035028890199e0f48db38642cb66a4181e028a6443a404fea284ce02b4614b683367d40874e505611d23142d49f0
6feea831d52d347b13610b413c4efc43a6de9f0b08d2a951dc503b6":MBEDTLS_RSA_PKCS_V15:2048:16:"e79a37
3182bfaa722eb035f772ad2a9464bd842de59432c18bbab3a7dfeae318c9b915ee487861ab665a40bd6cda560152578e

8579016c929df99fea05b4d64efca1d543850bc8164b40d71ed7f3fa4105df0fb9b9ad2a18ce182c8a4f4f975bea9aa0b9
a1438a27a28e97ac8330ef37383414d1bd64607d6979ac050424fd17":16:"c6749cbb0db8c5a177672d4728a8b22392b
2fc4d3b8361d5c0d5055a1b4e46d821f757c24eef2a51c561941b93b3ace7340074c058c9bb48e7e7414f42c41da4cccb
5c2ba91deb30c586b7fb18af12a52995592ad139d3be429add6547e044becedaf31fa3b39421e24ee034fbf367d11f6b8f
88ee483d163b431e1654ad3e89":16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6
ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace6890361
7faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a
7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cb
b448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8
c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"3":15:"4E636AF98E40F3ADCFCCB
698F4E80B9F":MBEDTLS_ERR_RSA_OUTPUT_TOO_LARGE

RSA
Check empty private key
rsa_check_privkey_null:

RSA
Check Private key #1 (Correct)
mbedtls_rsa_check_privkey:2048:16:"e79a373182bfaa722eb035f772ad2a9464bd842de59432c18bbab3a7dfeae318c
9b915ee487861ab665a40bd6cda560152578e8579016c929df99fea05b4d64efca1d543850bc8164b40d71ed7f3fa4105
df0fb9b9ad2a18ce182c8a4f4f975bea9aa0b9a1438a27a28e97ac8330ef37383414d1bd64607d6979ac050424fd17":16
:"c6749cbb0db8c5a177672d4728a8b22392b2fc4d3b8361d5c0d5055a1b4e46d821f757c24eef2a51c561941b93b3ace
7340074c058c9bb48e7e7414f42c41da4cccb5c2ba91deb30c586b7fb18af12a52995592ad139d3be429add6547e044b
ecedaf31fa3b39421e24ee034fbf367d11f6b8f88ee483d163b431e1654ad3e89":16:"b38ac65c8141f7f5c96e14470e85
1936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b976
9a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509
d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab2
03b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d
7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034
f":16:"3":16:"77B1D99300D6A54E864962DA09AE10CF19A7FB888456BC2672B72AEA52B204914493D16C18
4AD201EC3F762E1FBD8702BA796EF953D9EA2F26300D285264F11B0C8301D0207FEB1E2C984445C899B0
ACEBAA74EF014DD1D4BDDB43202C08D2FF9692D8D788478DEC829EB52AFB5AE068FBDBAC499A27FA
CECC391E75C936D55F07BB45EE184DAB45808E15722502F279F89B38C1CB292557E5063597F52C75D61001
EDC33F4739353E33E56AD273B067C1A2760208529EA421774A5FFFCB3423B1E0051E7702A55D80CBF2141
569F18F87BFF538A1DA8EDBB2693A539F68E0D62D77743F89EACF3B1723BDB25CE2F333FA63CACF0E67
DF1A431893BB9B352FCB":16:"9A66CF76572A71A17475794FA1C8C70D987E581E990D772BB27C77C53FF1
ECBB31260E9EDAFAEBC79991807E48918EAB8C3A5F03A600F30C69511546AE788EDF53168E2D035D300
EDCD5E4BF3AA2A6D603EA0A7BD11E1C1089657306DF8A64E7F1BC6B266B825C1A6C5F0FC85775F4CF7
ACD63367E42EAFE46511D58AD6DFE0F":16:"844DBDD20925D9164F9A1E2F707076C261CCA8337D024139
2B38AE3C12342F3AC14F8FD6DF4A1C36839662BD0D227344CD55A32AE5DBD2309A9A2B8A2C82BE6DD
DDCE81D1B694775D9047AA765CA0C6E1BB8E61C8B7BE27ED711E8EE2FEAD87F3491F76A6D2262C1418
9EACDFD4CEFE0BF9D0A5B49857E0ED22CBEB98DC8D45B":16:"4951A7B174DF972C37BADCC38457B5E
DD1F078BC613E75CE25E08814E12461C7A1C189A70EB8138294298D141244C7A9DE31AB4F6D38B40B04D
6353CD30F77ADBF66BBDE41C7BE463C5E30AAA3F7BAD6CEE99506DEAAFA2F335C1B1C5C88B8ABB0
D0387EE0D1B4E7027F7F085A025CEDB5CCE18B88C0462F1C3C910D47C0D4AB":0

RSA

Check Private key #2 (No P)

mbedtls_rsa_check_privkey:2048:16:"":16:"c6749cbb0db8c5a177672d4728a8b22392b2fc4d3b8361d5c0d5055a1b4e46d821f757c24eef2a51c561941b93b3ace7340074c058c9bb48e7e7414f42c41da4cccb5c2ba91deb30c586b7fb18af12a52995592ad139d3be429add6547e044becedaf31fa3b39421e24ee034fbf367d11f6b8f88ee483d163b431e1654ad3e89":16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"3":16:"77B1D99300D6A54E864962DA09AE10CF19A7FB888456BC2672B72AEA52B204914493D16C184AD201EC3F762E1FBD8702BA796EF953D9EA2F26300D285264F11B0C8301D0207FEB1E2C984445C899B0ACEBAA74EF014DD1D4BDDB43202C08D2FF9692D8D788478DEC829EB52AFB5AE068FBDBAC499A27FACECC391E75C936D55F07BB45EE184DAB45808E15722502F279F89B38C1CB292557E5063597F52C75D61001EDC33F4739353E33E56AD273B067C1A2760208529EA421774A5FFFCB3423B1E0051E7702A55D80CBF2141569F18F87BFF538A1DA8EDBB2693A539F68E0D62D77743F89EACF3B1723BDB25CE2F333FA63CACF0E67DF1A431893BB9B352FCB":16:"9A66CF76572A71A17475794FA1C8C70D987E581E990D772BB27C77C53FF1ECBB31260E9EDAFAEBC79991807E48918EAB8C3A5F03A600F30C69511546AE788EDF53168E2D035D300EDCD5E4BF3AA2A6D603EA0A7BD11E1C1089657306DF8A64E7F1BC6B266B825C1A6C5F0FC85775F4CF7ACD63367E42EAFE46511D58AD6DFE0F":16:"844DBDD20925D9164F9A1E2F707076C261CCA8337D0241392B38AE3C12342F3AC14F8FD6DF4A1C36839662BD0D227344CD55A32AE5DBD2309A9A2B8A2C82BE6DDDDCE81D1B694775D9047AA765CA0C6E1BB8E61C8B7BE27ED711E8EE2FEAD87F3491F76A6D2262C14189EACDFD4CEFE0BF9D0A5B49857E0ED22CBEB98DC8D45B":16:"4951A7B174DF972C37BADCC38457B5EDD1F078BC613E75CE25E08814E12461C7A1C189A70EB8138294298D141244C7A9DE31AB4F6D38B40B04D6353CD30F77ADBF66BBDE41C7BE463C5E30AAA3F7BAD6CEE99506DEAAFA2F335C1B1C5C88B8ABB0D0387EE0D1B4E7027F7F085A025CEDB5CCE18B88C0462F1C3C910D47C0D4AB":MBEDTLS_ERR_RSA_KEY_CHECK_FAILED

RSA

Check Private key #3 (No Q)

mbedtls_rsa_check_privkey:2048:16:"e79a373182bfaa722eb035f772ad2a9464bd842de59432c18bbab3a7dfeae318c9b915ee487861ab665a40bd6cda560152578e8579016c929df99fea05b4d64efca1d543850bc8164b40d71ed7f3fa4105df0fb9b9ad2a18ce182c8a4f4f975bea9aa0b9a1438a27a28e97ac8330ef37383414d1bd64607d6979ac050424fd17":16:"":16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"3":16:"77B1D99300D6A54E864962DA09AE10CF19A7FB888456BC2672B72AEA52B204914493D16C184AD201EC3F762E1FBD8702BA796EF953D9EA2F26300D285264F11B0C8301D0207FEB1E2C984445C899B0ACEBAA74EF014DD1D4BDDB43202C08D2FF9692D8D788478DEC829EB52AFB5AE068FBDBAC499A27FACECC391E75C936D55F07BB45EE184DAB45808E15722502F279F89B38C1CB292557E5063597F52C75D61001EDC33F4739353E33E56AD273B067C1A2760208529EA421774A5FFFCB3423B1E0051E7702A55D80CBF2141569F18F87BFF538A1DA8EDBB2693A539F68E0D62D77743F89EACF3B1723BDB25CE2F333FA63CACF0E67DF1A431893BB9B352FCB":16:"9A66CF76572A71A17475794FA1C8C70D987E581E990D772BB27C77C53FF1ECBB31260E9EDAFAEBC79991807E48918EAB8C3A5F03A600F30C69511546AE788EDF53168E2D035D300EDCD5E4BF3AA2A6D603EA0A7BD11E1C1089657306DF8A64E7F1BC6B266B825C1A6C5F0FC85775F4CF7ACD63367E42EAFE46511D58AD6DFE0F":16:"844DBDD20925D9164F9A1E2F707076C261CCA8337D0241392B38AE3C12342F3AC14F8FD6DF4A1C36839662BD0D227344CD55

A32AE5DBD2309A9A2B8A2C82BE6DDDDCE81D1B694775D9047AA765CA0C6E1BB8E61C8B7BE27ED711
E8EE2FEAD87F3491F76A6D2262C14189EACDFD4CEFE0BF9D0A5B49857E0ED22CBEB98DC8D45B":16:"4
951A7B174DF972C37BADCC38457B5EDD1F078BC613E75CE25E08814E12461C7A1C189A70EB8138294298
D141244C7A9DE31AB4F6D38B40B04D6353CD30F77ADBF66BBDE41C7BE463C5E30AAA3F7BAD6CEE99
506DEAAFA2F335C1B1C5C88B8ABB0D0387EE0D1B4E7027F7F085A025CEDB5CCE18B88C0462F1C3C910
D47C0D4AB":MBEDTLS_ERR_RSA_KEY_CHECK_FAILED

RSA

Check Private key #4 (No N)

mbedtls_rsa_check_privkey:2048:16:"e79a373182bfaa722eb035f772ad2a9464bd842de59432c18bbab3a7dfeae318c
9b915ee487861ab665a40bd6cda560152578e8579016c929df99fea05b4d64efca1d543850bc8164b40d71ed7f3fa4105
df0fb9b9ad2a18ce182c8a4f4f975bea9aa0b9a1438a27a28e97ac8330ef37383414d1bd64607d6979ac050424fd17":16
:"c6749cbb0db8c5a177672d4728a8b22392b2fc4d3b8361d5c0d5055a1b4e46d821f757c24eef2a51c561941b93b3ace
7340074c058c9bb48e7e7414f42c41da4cccb5c2ba91deb30c586b7fb18af12a52995592ad139d3be429add6547e044b
ecedaf31fa3b39421e24ee034fbf367d11f6b8f88ee483d163b431e1654ad3e89":16:"":16:"3":16:"77B1D99300D6A54
E864962DA09AE10CF19A7FB888456BC2672B72AEA52B204914493D16C184AD201EC3F762E1FBD8702BA
796EF953D9EA2F26300D285264F11B0C8301D0207FEB1E2C984445C899B0ACEBAA74EF014DD1D4BDDB4
3202C08D2FF9692D8D788478DEC829EB52AFB5AE068FBDBAC499A27FACECC391E75C936D55F07BB45E
E184DAB45808E15722502F279F89B38C1CB292557E5063597F52C75D61001EDC33F4739353E33E56AD273B
067C1A2760208529EA421774A5FFFCB3423B1E0051E7702A55D80CBF2141569F18F87BFF538A1DA8EDBB
2693A539F68E0D62D77743F89EACF3B1723BDB25CE2F333FA63CACF0E67DF1A431893BB9B352FCB":16:"
9A66CF76572A71A17475794FA1C8C70D987E581E990D772BB27C77C53FF1ECBB31260E9EDAFAEBC7999
1807E48918EAB8C3A5F03A600F30C69511546AE788EDF53168E2D035D300EDCD5E4BF3AA2A6D603EA0A
7BD11E1C1089657306DF8A64E7F1BC6B266B825C1A6C5F0FC85775F4CF7ACD63367E42EAFE46511D58A
D6DFE0F":16:"844DBDD20925D9164F9A1E2F707076C261CCA8337D0241392B38AE3C12342F3AC14F8FD6
DF4A1C36839662BD0D227344CD55A32AE5DBD2309A9A2B8A2C82BE6DDDDCE81D1B694775D9047AA7
65CA0C6E1BB8E61C8B7BE27ED711E8EE2FEAD87F3491F76A6D2262C14189EACDFD4CEFE0BF9D0A5B4
9857E0ED22CBEB98DC8D45B":16:"4951A7B174DF972C37BADCC38457B5EDD1F078BC613E75CE25E0881
4E12461C7A1C189A70EB8138294298D141244C7A9DE31AB4F6D38B40B04D6353CD30F77ADBF66BBDE41
C7BE463C5E30AAA3F7BAD6CEE99506DEAAFA2F335C1B1C5C88B8ABB0D0387EE0D1B4E7027F7F085A0
25CEDB5CCE18B88C0462F1C3C910D47C0D4AB":MBEDTLS_ERR_RSA_KEY_CHECK_FAILED

RSA

Check Private key #5 (No E)

mbedtls_rsa_check_privkey:2048:16:"e79a373182bfaa722eb035f772ad2a9464bd842de59432c18bbab3a7dfeae318c
9b915ee487861ab665a40bd6cda560152578e8579016c929df99fea05b4d64efca1d543850bc8164b40d71ed7f3fa4105
df0fb9b9ad2a18ce182c8a4f4f975bea9aa0b9a1438a27a28e97ac8330ef37383414d1bd64607d6979ac050424fd17":16
:"c6749cbb0db8c5a177672d4728a8b22392b2fc4d3b8361d5c0d5055a1b4e46d821f757c24eef2a51c561941b93b3ace
7340074c058c9bb48e7e7414f42c41da4cccb5c2ba91deb30c586b7fb18af12a52995592ad139d3be429add6547e044b
ecedaf31fa3b39421e24ee034fbf367d11f6b8f88ee483d163b431e1654ad3e89":16:"b38ac65c8141f7f5c96e14470e85
1936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b976
9a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509
d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab2
03b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d
7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034
f":16:"":16:"77B1D99300D6A54E864962DA09AE10CF19A7FB888456BC2672B72AEA52B204914493D16C184
AD201EC3F762E1FBD8702BA796EF953D9EA2F26300D285264F11B0C8301D0207FEB1E2C984445C899B0A
CEBAA74EF014DD1D4BDDB43202C08D2FF9692D8D788478DEC829EB52AFB5AE068FBDBAC499A27FAC

ECC391E75C936D55F07BB45EE184DAB45808E15722502F279F89B38C1CB292557E5063597F52C75D61001E
DC33F4739353E33E56AD273B067C1A2760208529EA421774A5FFFCB3423B1E0051E7702A55D80CBF21415
69F18F87BFF538A1DA8EDBB2693A539F68E0D62D77743F89EACF3B1723BDB25CE2F333FA63CACF0E67
DF1A431893BB9B352FCB":16:"9A66CF76572A71A17475794FA1C8C70D987E581E990D772BB27C77C53FF1
ECBB31260E9EDAFAEBC79991807E48918EAB8C3A5F03A600F30C69511546AE788EDF53168E2D035D300
EDCD5E4BF3AA2A6D603EA0A7BD11E1C1089657306DF8A64E7F1BC6B266B825C1A6C5F0FC85775F4CF7
ACD63367E42EAFE46511D58AD6DFE0F":16:"844DBDD20925D9164F9A1E2F707076C261CCA8337D024139
2B38AE3C12342F3AC14F8FD6DF4A1C36839662BD0D227344CD55A32AE5DBD2309A9A2B8A2C82BE6DD
DDCE81D1B694775D9047AA765CA0C6E1BB8E61C8B7BE27ED711E8EE2FEAD87F3491F76A6D2262C1418
9EACDFD4CEFE0BF9D0A5B49857E0ED22CBEB98DC8D45B":16:"4951A7B174DF972C37BADCC38457B5E
DD1F078BC613E75CE25E08814E12461C7A1C189A70EB8138294298D141244C7A9DE31AB4F6D38B40B04D
6353CD30F77ADBF66BBDE41C7BE463C5E30AAA3F7BAD6CEE99506DEAAFA2F335C1B1C5C88B8ABB0
D0387EE0D1B4E7027F7F085A025CEDB5CCE18B88C0462F1C3C910D47C0D4AB":MBEDTLS_ERR_RSA_K
EY_CHECK_FAILED

RSA
Check Private key #6 (No D)
mbedtls_rsa_check_privkey:2048:16:"e79a373182bfaa722eb035f772ad2a9464bd842de59432c18bbab3a7dfeae318c
9b915ee487861ab665a40bd6cda560152578e8579016c929df99fea05b4d64efca1d543850bc8164b40d71ed7f3fa4105
df0fb9b9ad2a18ce182c8a4f4f975bea9aa0b9a1438a27a28e97ac8330ef37383414d1bd64607d6979ac050424fd17":16
:"c6749cbb0db8c5a177672d4728a8b22392b2fc4d3b8361d5c0d5055a1b4e46d821f757c24eef2a51c561941b93b3ace
7340074c058c9bb48e7e7414f42c41da4cccb5c2ba91deb30c586b7fb18af12a52995592ad139d3be429add6547e044b
ecedaf31fa3b39421e24ee034fbf367d11f6b8f88ee483d163b431e1654ad3e89":16:"b38ac65c8141f7f5c96e14470e85
1936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b976
9a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509
d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab2
03b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d
7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034
f":16:"3":16:"":16:"9A66CF76572A71A17475794FA1C8C70D987E581E990D772BB27C77C53FF1ECBB31260E
9EDAFAEBC79991807E48918EAB8C3A5F03A600F30C69511546AE788EDF53168E2D035D300EDCD5E4BF3
AA2A6D603EA0A7BD11E1C1089657306DF8A64E7F1BC6B266B825C1A6C5F0FC85775F4CF7ACD63367E42
EAFE46511D58AD6DFE0F":16:"844DBDD20925D9164F9A1E2F707076C261CCA8337D0241392B38AE3C123
42F3AC14F8FD6DF4A1C36839662BD0D227344CD55A32AE5DBD2309A9A2B8A2C82BE6DDDDCE81D1B6
94775D9047AA765CA0C6E1BB8E61C8B7BE27ED711E8EE2FEAD87F3491F76A6D2262C14189EACDFD4CE
FE0BF9D0A5B49857E0ED22CBEB98DC8D45B":16:"4951A7B174DF972C37BADCC38457B5EDD1F078BC61
3E75CE25E08814E12461C7A1C189A70EB8138294298D141244C7A9DE31AB4F6D38B40B04D6353CD30F77
ADBF66BBDE41C7BE463C5E30AAA3F7BAD6CEE99506DEAAFA2F335C1B1C5C88B8ABB0D0387EE0D1B
4E7027F7F085A025CEDB5CCE18B88C0462F1C3C910D47C0D4AB":MBEDTLS_ERR_RSA_KEY_CHECK_F
AILED

RSA
Check Private key #7 (No DP)
mbedtls_rsa_check_privkey:2048:16:"e79a373182bfaa722eb035f772ad2a9464bd842de59432c18bbab3a7dfeae318c
9b915ee487861ab665a40bd6cda560152578e8579016c929df99fea05b4d64efca1d543850bc8164b40d71ed7f3fa4105
df0fb9b9ad2a18ce182c8a4f4f975bea9aa0b9a1438a27a28e97ac8330ef37383414d1bd64607d6979ac050424fd17":16
:"c6749cbb0db8c5a177672d4728a8b22392b2fc4d3b8361d5c0d5055a1b4e46d821f757c24eef2a51c561941b93b3ace
7340074c058c9bb48e7e7414f42c41da4cccb5c2ba91deb30c586b7fb18af12a52995592ad139d3be429add6547e044b
ecedaf31fa3b39421e24ee034fbf367d11f6b8f88ee483d163b431e1654ad3e89":16:"b38ac65c8141f7f5c96e14470e85

1936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b976
9a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509
d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab2
03b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d
7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034
f":16:"3":16:"77B1D99300D6A54E864962DA09AE10CF19A7FB888456BC2672B72AEA52B204914493D16C18
4AD201EC3F762E1FBD8702BA796EF953D9EA2F26300D285264F11B0C8301D0207FEB1E2C984445C899B0
ACEBAA74EF014DD1D4BDDB43202C08D2FF9692D8D788478DEC829EB52AFB5AE068FBDBAC499A27FA
CECC391E75C936D55F07BB45EE184DAB45808E15722502F279F89B38C1CB292557E5063597F52C75D61001
EDC33F4739353E33E56AD273B067C1A2760208529EA421774A5FFFCB3423B1E0051E7702A55D80CBF2141
569F18F87BFF538A1DA8EDBB2693A539F68E0D62D77743F89EACF3B1723BDB25CE2F333FA63CACF0E67
DF1A431893BB9B352FCB":16:"":16:"844DBDD20925D9164F9A1E2F707076C261CCA8337D0241392B38AE3
C12342F3AC14F8FD6DF4A1C36839662BD0D227344CD55A32AE5DBD2309A9A2B8A2C82BE6DDDDCE81
D1B694775D9047AA765CA0C6E1BB8E61C8B7BE27ED711E8EE2FEAD87F3491F76A6D2262C14189EACDF
D4CEFE0BF9D0A5B49857E0ED22CBEB98DC8D45B":16:"4951A7B174DF972C37BADCC38457B5EDD1F078
BC613E75CE25E08814E12461C7A1C189A70EB8138294298D141244C7A9DE31AB4F6D38B40B04D6353CD3
0F77ADBF66BBDE41C7BE463C5E30AAA3F7BAD6CEE99506DEAAFA2F335C1B1C5C88B8ABB0D0387EE0
D1B4E7027F7F085A025CEDB5CCE18B88C0462F1C3C910D47C0D4AB":MBEDTLS_ERR_RSA_KEY_CHEC
K_FAILED

RSA
Check Private key #8 (No DQ)
mbedtls_rsa_check_privkey:2048:16:"e79a373182bfaa722eb035f772ad2a9464bd842de59432c18bbab3a7dfeae318c
9b915ee487861ab665a40bd6cda560152578e8579016c929df99fea05b4d64efca1d543850bc8164b40d71ed7f3fa4105
df0fb9b9ad2a18ce182c8a4f4f975bea9aa0b9a1438a27a28e97ac8330ef37383414d1bd64607d6979ac050424fd17":16
:"c6749cbb0db8c5a177672d4728a8b22392b2fc4d3b8361d5c0d5055a1b4e46d821f757c24eef2a51c561941b93b3ace
7340074c058c9bb48e7e7414f42c41da4cccb5c2ba91deb30c586b7fb18af12a52995592ad139d3be429add6547e044b
ecedaf31fa3b39421e24ee034fbf367d11f6b8f88ee483d163b431e1654ad3e89":16:"b38ac65c8141f7f5c96e14470e85
1936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b976
9a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509
d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab2
03b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d
7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034
f":16:"3":16:"77B1D99300D6A54E864962DA09AE10CF19A7FB888456BC2672B72AEA52B204914493D16C18
4AD201EC3F762E1FBD8702BA796EF953D9EA2F26300D285264F11B0C8301D0207FEB1E2C984445C899B0
ACEBAA74EF014DD1D4BDDB43202C08D2FF9692D8D788478DEC829EB52AFB5AE068FBDBAC499A27FA
CECC391E75C936D55F07BB45EE184DAB45808E15722502F279F89B38C1CB292557E5063597F52C75D61001
EDC33F4739353E33E56AD273B067C1A2760208529EA421774A5FFFCB3423B1E0051E7702A55D80CBF2141
569F18F87BFF538A1DA8EDBB2693A539F68E0D62D77743F89EACF3B1723BDB25CE2F333FA63CACF0E67
DF1A431893BB9B352FCB":16:"9A66CF76572A71A17475794FA1C8C70D987E581E990D772BB27C77C53FF1
ECBB31260E9EDAFAEBC79991807E48918EAB8C3A5F03A600F30C69511546AE788EDF53168E2D035D300
EDCD5E4BF3AA2A6D603EA0A7BD11E1C1089657306DF8A64E7F1BC6B266B825C1A6C5F0FC85775F4CF7
ACD63367E42EAFE46511D58AD6DFE0F":16:"":16:"4951A7B174DF972C37BADCC38457B5EDD1F078BC61
3E75CE25E08814E12461C7A1C189A70EB8138294298D141244C7A9DE31AB4F6D38B40B04D6353CD30F77
ADBF66BBDE41C7BE463C5E30AAA3F7BAD6CEE99506DEAAFA2F335C1B1C5C88B8ABB0D0387EE0D1B
4E7027F7F085A025CEDB5CCE18B88C0462F1C3C910D47C0D4AB":MBEDTLS_ERR_RSA_KEY_CHECK_F
AILED

RSA

Check Private key #9 (No QP)

mbedtls_rsa_check_privkey:2048:16:"e79a373182bfaa722eb035f772ad2a9464bd842de59432c18bbab3a7dfeae318c9b915ee487861ab665a40bd6cda560152578e8579016c929df99fea05b4d64efca1d543850bc8164b40d71ed7f3fa4105df0fb9b9ad2a18ce182c8a4f4f975bea9aa0b9a1438a27a28e97ac8330ef37383414d1bd64607d6979ac050424fd17":16:"c6749cbb0db8c5a177672d4728a8b22392b2fc4d3b8361d5c0d5055a1b4e46d821f757c24eef2a51c561941b93b3ace7340074c058c9bb48e7e7414f42c41da4cccb5c2ba91deb30c586b7fb18af12a52995592ad139d3be429add6547e044becedaf31fa3b39421e24ee034fbf367d11f6b8f88ee483d163b431e1654ad3e89":16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"3":16:"77B1D99300D6A54E864962DA09AE10CF19A7FB888456BC2672B72AEA52B204914493D16C184AD201EC3F762E1FBD8702BA796EF953D9EA2F26300D285264F11B0C8301D0207FEB1E2C984445C899B0ACEBAA74EF014DD1D4BDDB43202C08D2FF9692D8D788478DEC829EB52AFB5AE068FBDBAC499A27FACECC391E75C936D55F07BB45EE184DAB45808E15722502F279F89B38C1CB292557E5063597F52C75D61001EDC33F4739353E33E56AD273B067C1A2760208529EA421774A5FFFCB3423B1E0051E7702A55D80CBF2141569F18F87BFF538A1DA8EDBB2693A539F68E0D62D77743F89EACF3B1723BDB25CE2F333FA63CACF0E67DF1A431893BB9B352FCB":16:"9A66CF76572A71A17475794FA1C8C70D987E581E990D772BB27C77C53FF1ECBB31260E9EDAFAEBC79991807E48918EAB8C3A5F03A600F30C69511546AE788EDF53168E2D035D300EDCD5E4BF3AA2A6D603EA0A7BD11E1C1089657306DF8A64E7F1BC6B266B825C1A6C5F0FC85775F4CF7ACD63367E42EAFE46511D58AD6DFE0F":16:"844DBDD20925D9164F9A1E2F707076C261CCA8337D0241392B38AE3C12342F3AC14F8FD6DF4A1C36839662BD0D227344CD55A32AE5DBD2309A9A2B8A2C82BE6DDDDCE81D1B694775D9047AA765CA0C6E1BB8E61C8B7BE27ED711E8EE2FEAD87F3491F76A6D2262C14189EACDFD4CEFE0BF9D0A5B49857E0ED22CBEB98DC8D45B":16:"":MBEDTLS_ERR_RSA_KEY_CHECK_FAILED

RSA

Check Private key #10 (Incorrect)

mbedtls_rsa_check_privkey:2048:16:"e79a373182bfaa722eb035f772ad2a9464bd842de59432c18bbab3a7dfeae318c9b915ee487861ab665a40bd6cda560152578e8579016c929df99fea05b4d64efca1d543850bc8164b40d71ed7f3fa4105df0fb9b9ad2a18ce182c8a4f4f975bea9aa0b9a1438a27a28e97ac8330ef37383414d1bd64607d6979ac050424fd17":16:"c6749cbb0db8c5a177672d4728a8b22392b2fc4d3b8361d5c0d5055a1b4e46d821f757c24eef2a51c561941b93b3ace7340074c058c9bb48e7e7414f42c41da4cccb5c2ba91deb30c586b7fb18af12a52995592ad139d3be429add6547e044becedaf31fa3b39421e24ee034fbf367d11f6b8f88ee483d163b431e1654ad3e89":16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"3":16:"77B1D99300D6A54E864962DA09AE10CF19A7FB888456BC2672B72AEA52B204914493D16C184AD201EC3F762E1FBD8702BA796EF953D9EA2F26300D285264F11B0C8301D0207FEB1E2C984445C899B0ACEBAA74EF014DD1D4BDDB43202C08D2FF9692D8D788478DEC829EB52AFB5AE068FBDBAC499A27FACECC391E75C936D55F07BB45EE184DAB45808E15722502F279F89B38C1CB292557E5063597F52C75D61001EDC33F4739353E33E56AD273B067C1A2760208529EA421774A5FFFCB3423B1E0051E7702A55D80CBF2141569F18F87BFF538A1DA8EDBB2693A539F68E0D62D77743F89EACF3B1723BDB25CE2F333FA63CACF0E67DF1A431893BB9B352FCC":16:"9A66CF76572A71A17475794FA1C8C70D987E581E990D772BB27C77C53FF1

ECBB31260E9EDAFAEBC79991807E48918EAB8C3A5F03A600F30C69511546AE788EDF53168E2D035D300EDCD5E4BF3AA2A6D603EA0A7BD11E1C1089657306DF8A64E7F1BC6B266B825C1A6C5F0FC85775F4CF7ACD63367E42EAFE46511D58AD6DFE0F":16:"844DBDD20925D9164F9A1E2F707076C261CCA8337D0241392B38AE3C12342F3AC14F8FD6DF4A1C36839662BD0D227344CD55A32AE5DBD2309A9A2B8A2C82BE6DDDDCE81D1B694775D9047AA765CA0C6E1BB8E61C8B7BE27ED711E8EE2FEAD87F3491F76A6D2262C14189EACDFD4CEFE0BF9D0A5B49857E0ED22CBEB98DC8D45B":16:"4951A7B174DF972C37BADCC38457B5EDD1F078BC613E75CE25E08814E12461C7A1C189A70EB8138294298D141244C7A9DE31AB4F6D38B40B04D6353CD30F77ADBF66BBDE41C7BE463C5E30AAA3F7BAD6CEE99506DEAAFA2F335C1B1C5C88B8ABB0D0387EE0D1B4E7027F7F085A025CEDB5CCE18B88C0462F1C3C910D47C0D4AB":MBEDTLS_ERR_RSA_KEY_CHECK_FAILED

RSA
Check Public key #1 (Correct)
mbedtls_rsa_check_pubkey:16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"3":0

RSA Check Public key #2 (Even N)
mbedtls_rsa_check_pubkey:16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a20340":16:"3":MBEDTLS_ERR_RSA_KEY_CHECK_FAILED

RSA
Check Public key #3 (Even E)
mbedtls_rsa_check_pubkey:16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a20340":16:"65536":MBEDTLS_ERR_RSA_KEY_CHECK_FAILED

RSA
Check Public key #4 (N exactly 128 bits)
mbedtls_rsa_check_pubkey:16:"fedcba9876543210deadbeefcafe4321":16:"3":0

RSA Check Public key #5 (N smaller than 128 bits)
mbedtls_rsa_check_pubkey:16:"7edcba9876543210deadbeefcafe4321":16:"3":MBEDTLS_ERR_RSA_KEY_CHECK_FAILED

RSA Check Public key #6 (N exactly 8192 bits)

mbedtls_rsa_check_pubkey:16:"88F48075BF29E95C1C6AE8716678B74E957B69CC2E49708C160C6343AAD2F
076D25397ACE74220311ED18AEEB681F463611B3340C3945CAAEAD3ACC616E08A25A55683A32979BD55
EA5DAB7630AF393886896F11DDC5F07E15EDF949324CF0F0B2A5C0E85DFA23167193182D1A43079DC864
5F6C2C029629F475575802F7D326DE5BD891A9C5F84A433D45154181EC05685A4B368A5B6434775A00ABC
6B0A04647D4598CEEE566B552230F691C98CA30B402A76C686A94B373CCD2F60EFA3878A867BB5F585D0
88E27C507937262D098A477B9218BE7C03B2E4C102D244CA701645F1827CD947E5E796446378B848862E68
9F0D1773F752056841A1F0EECE7CAB74921A42DBF2EF264ADCF4ABE05A1242E5F629A657A2D67958A2D
AC9A2245074A37099B45064723ABE21241058252632C2BA6FE85AB1C75FF310891B84C9C40AB646FE1D90
BC716FB3A4B56DA3EA25CA397C04B994F7C6AD1DD0CB9E994CA6B835F7830F4F4E0F976BBEA5AE855
6BC7C90B3E50E21C19AD1F6BC4A8FF15F2909D9CC5F3DA533BADFF50F487869D631C3E34D69636B4C25
A55127EF5B715F2FC0565734B38DF996D1970E56F7F64EBECB9D00A587AAEC608F2D3AAA51E66BF53E9
2C3096BF78D1DCBCE1A645FA4F0542E6F68E5A94AAA6E839F75620FABED5D2BCF40AB8EAF95F838BF
A962429F281578882DF0F2721C27C8905C9E776B1D3251FC066A8BC64C0CE7FBA2B8E21F65EF6739AB6F1
9EC2AB07817DFF03DAB7C846AB5CC86C103642D7664A85DC2D846A8004CD6A144C72CCCAC86DB5901
A047324927B80E281F5F7315FA2F9083BDE0DB7AA46DC055E36BB73FB6DBD3A14759D06CBBE8D57CBC
213C4D55DE4478679E0A5902C8655BE1391C0E88D2B1FBD57E9232A2CEBC67569ECD94E4BF0FCC6C003
F9AA51A2A5E6EE084A46DAE65E52400A727F9713D29E92CD6CA37FD599598B3F677624A2A484A8B36B9
8EFEAD662C0A23BC1D9280EF2A31F887065EB20A93B41F7A264ECFA65B3555F3E400927018186EAA2D4F
00C6B7AB1BCED5F893D64478177592C7F2B945307AB474D7EC7FF2E7E55834CC763BEF81DA9BD70FB3D
423AE5ADB86B336734C8A3BEC90CEB05438B5BA030D0D30DEC1442D2EB08450480FBAE090FFA1A5AD
D748A415BDCDE45094E792420F0AF94BCA0A80A2096D1A478D3428A214A7E68C0F07F58C6FB232ECC3
D8B821AE29AE76E13EB751193F6ECA670016D54F3D796937DDBB8900062EF116CCA3F5B3AECA6182728
75336C9C050FBC0FC7EDD5B88D85DA0061D21E176E1419CF573629BE7B0496E761EAD45FE32B59EB00D
47CDD178AC8F8EC8D6F26DED34F7576CD938422E18E936F16A704B483A48EE3BEA59D95F688136119894
930EC8E9282E5974740CF031DF8DBB07EB08F2DA0ACCADECE15A6A57502890F4A03740E60BD":16:"010
001":0

RSA

Check Public key #7 (N larger than 8192 bits)

mbedtls_rsa_check_pubkey:16:"01631CD83F3F2D67FA52E13B44416EA65043A322ECD65467558EACD4C6B6
D92DA7471D2DBD58E6921F9465C4900E92DFC6EB35C90637285A7E1F3D27C1C32FD6A5CB324D8253C6B
2E480B63F66E3B09F4300C3E683011C7803BDEAD682F0F55473FC8A187734573A11ECDCE802022F539BC2
074E94703C23E48FF8AE35702352E70AF921B42E6A143A3EFEE20DF77A97AA703AA271CE96EB78062452
D87A4ADCACF83FFB9683818BF2ED234D0ECFB1B935827708050C4D007215D7A028152798045AF6A0B741
A7B22F3FCCEBC26D285B9AA22CEF858858702BAE7D945FA0C45E2D8AADFF2FD0A64DF02C241F871C7
99AD73738E626D9A6D4BFFBCE000C4087F0CE74EF21526402FDCD07649175122697FD01041B84AD0A3FE
DABD5C25E953686B2272F8C8B748A486F54CB767A1C79CA499B2C9A300AC8A214A0BFA06280A9235D5
B7AFB8A76FFDD78FC72038C5B809569A6125D6A588684A16D222EF93F2469EA78948037957DE9B449AB7
22044FDFF3B6AC89367D72F0CF3ED1F85EDFD0DE3EEEDD39F6EFD68A0368F83B389B7A7B9C7713F4148
F53E82CDF6D9CC002A3A16F1E6A1D78C48CE784958416466166415 3A499ACAE5927728B2F1A2E91164867
6DF316DFCBF5E44F393B7B296A4A21ED59744E3855FCD4A21F2B42CFE5C52860B244D467103107E3DC40
A82077269897528CCBF80B2F216A535C52A6A2643E64B53276A1B63348038706328FE369AE2409568160481
C07A3ED5B0198EC6CC07F8F250B1DE0D97110F834AA3D1C0862FB719393EA08D530225CE0647FD5488F4
83FA065196D1160FAFA54CD3FF63B6ADDBE84D09F3CFF98F22CC71DE2FC19735126C3BBA9A2C293D1D
B118F0512C144C1C616492BE0D19BFD245955840F640EBE6FCFF2830C683852046F36C3CDA4F4460ABA4B
2FEEB700C9DD80418C42673858CDD11E70682D5A41ED7D8010EC7DD5B57B4E206F84DB8A430B246002F
EA49AFF45940B1F18AE28863F5AA41D3B42ABCD3D1BAB7644B86E060865997E1BA23A768F233D8A8593
32F8B9D5D1633F9C462328C17E2B07D6DFD813C94D675873592E5CBB001C112A790B10B9F9E07BE105C4

FD328C7E3887C3EF13E8ECE6106B73A3341AF200D8663BDF96FFDB6F794FBB04D976B87423A868882F15
CAE8DC9F6CAF4917EFC844E74BAD48F21E34530CB4E20006444706FC95658735553CA99E18F0E820D78D
EF8FB84034B10CE44B1AE36B50147558415E5E78A77E2FC7C8C580B54CCC40EE3904C04950846A6D51BF
5C80E0B6E2ADC4989DA1D3DD01F99AA369C2E6B53394BA0CB5E6E811BFA004A5B3B3C34C60433AB5E
B0EC8050246B9AF10B49EAA51487CCE0C4C8F4CDAF926D582D7E4924C33765E00AC952A38669150EA32
2CDF886B46DE4D0970A060B670D50C9BF3D2020B529838E192EF92BFE2F06FDF1D5":16:"010001":MBED
TLS_ERR_RSA_KEY_CHECK_FAILED

RSA
Check Public key #8 (E exactly 2 bits)
mbedtls_rsa_check_pubkey:16:"fedcba9876543210deadbeefcafe4321":16:"3":0

RSA Check Public key #8 (E exactly 1 bits)
mbedtls_rsa_check_pubkey:16:"fedcba9876543210deadbeefcafe4321":16:"1":MBEDTLS_ERR_RSA_KEY_CHE
CK_FAILED

RSA Check Public key #8 (E exactly 64 bits)
mbedtls_rsa_check_pubkey:16:"fedcba9876543210deadbeefcafe4321":16:"00fedcba9876543213":0

RSA Check
Public key #8 (E larger than 64 bits)
mbedtls_rsa_check_pubkey:16:"fedcba9876543210deadbeefcafe4321":16:"01fedcba9876543213":0

RSA Check Public key #9 (E has size N-2)
mbedtls_rsa_check_pubkey:16:"00b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6dd
ba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617fa
f6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bc
d1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb4
48de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c2
3893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034fb38ac65c8141f7f5c96e14470e851936a67bf9
4cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b
830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e6
73bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b352557
65261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97
daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"00b3
8ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b
62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc4
5434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec5955
9dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d3
91ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f355
49141486c3b0961a7b4c1a2034fb38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba
2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6
681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1
b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448
de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c238
93d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034d":0

RSA

Check Public key #10 (E has size N)

mbedtls_rsa_check_pubkey:16:"00b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034fb38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"00b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":MBEDTLS_ERR_RSA_KEY_CHECK_FAILED

RSA

Check Public-Private key #1 (Correct)

rsa_check_pubpriv:2048:16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"3":16:"e79a373182bfaa722eb035f772ad2a9464bd842de59432c18bbab3a7dfeae318c9b915ee487861ab665a40bd6cda560152578e8579016c929df99fea05b4d64efca1d543850bc8164b40d71ed7f3fa4105df0fb9b9ad2a18ce182c8a4f4f975bea9aa0b9a1438a27a28e97ac8330ef37383414d1bd64607d6979ac050424fd17":16:"c6749cbb0db8c5a177672d4728a8b22392b2fc4d3b8361d5c0d5055a1b4e46d821f757c24eef2a51c561941b93b3ace7340074c058c9bb48e7e7414f42c41da4cccb5c2ba91deb30c586b7fb18af12a52995592ad139d3be429add6547e044becedaf31fa3b39421e24ee034fbf367d11f6b8f88ee483d163b431e1654ad3e89":16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"3":16:"77B1D99300D6A54E864962DA09AE10CF19A7FB888456BC2672B72AEA52B204914493D16C184AD201EC3F762E1FBD8702BA796EF953D9EA2F26300D285264F11B0C8301D0207FEB1E2C984445C899B0ACEBAA74EF014DD1D4BDDB43202C08D2FF9692D8D788478DEC829EB52AFB5AE068FBDBAC499A27FACECC391E75C936D55F07BB45EE184DAB45808E15722502F279F89B38C1CB292557E5063597F52C75D61001EDC33F4739353E33E56AD273B067C1A2760208529EA421774A5FFF

CB3423B1E0051E7702A55D80CBF2141569F18F87BFF538A1DA8EDBB2693A539F68E0D62D77743F89EACF
3B1723BDB25CE2F333FA63CACF0E67DF1A431893BB9B352FCB":16:"9A66CF76572A71A17475794FA1C8
C70D987E581E990D772BB27C77C53FF1ECBB31260E9EDAFAEBC79991807E48918EAB8C3A5F03A600F30
C69511546AE788EDF53168E2D035D300EDCD5E4BF3AA2A6D603EA0A7BD11E1C1089657306DF8A64E7F1
BC6B266B825C1A6C5F0FC85775F4CF7ACD63367E42EAFE46511D58AD6DFE0F":16:"844DBDD20925D916
4F9A1E2F707076C261CCA8337D0241392B38AE3C12342F3AC14F8FD6DF4A1C36839662BD0D227344CD55
A32AE5DBD2309A9A2B8A2C82BE6DDDDCE81D1B694775D9047AA765CA0C6E1BB8E61C8B7BE27ED711
E8EE2FEAD87F3491F76A6D2262C14189EACDFD4CEFE0BF9D0A5B49857E0ED22CBEB98DC8D45B":16:"4
951A7B174DF972C37BADCC38457B5EDD1F078BC613E75CE25E08814E12461C7A1C189A70EB8138294298
D141244C7A9DE31AB4F6D38B40B04D6353CD30F77ADBF66BBDE41C7BE463C5E30AAA3F7BAD6CEE99
506DEAAFA2F335C1B1C5C88B8ABB0D0387EE0D1B4E7027F7F085A025CEDB5CCE18B88C0462F1C3C910
D47C0D4AB":0

RSA

Check Public-Private key #2 (Public no N)

rsa_check_pubpriv:2048:16:"":16:"3":16:"e79a373182bfaa722eb035f772ad2a9464bd842de59432c18bbab3a7dfeae
318c9b915ee487861ab665a40bd6cda560152578e8579016c929df99fea05b4d64efca1d543850bc8164b40d71ed7f3fa
4105df0fb9b9ad2a18ce182c8a4f4f975bea9aa0b9a1438a27a28e97ac8330ef37383414d1bd64607d6979ac050424fd1
7":16:"c6749cbb0db8c5a177672d4728a8b22392b2fc4d3b8361d5c0d5055a1b4e46d821f757c24eef2a51c561941b93
b3ace7340074c058c9bb48e7e7414f42c41da4cccb5c2ba91deb30c586b7fb18af12a52995592ad139d3be429add6547e
044becedaf31fa3b39421e24ee034fbf367d11f6b8f88ee483d163b431e1654ad3e89":16:"b38ac65c8141f7f5c96e1447
0e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7
b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc0790
8509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eaf
bdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810
c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c
1a2034f":16:"3":16:"77B1D99300D6A54E864962DA09AE10CF19A7FB888456BC2672B72AEA52B204914493
D16C184AD201EC3F762E1FBD8702BA796EF953D9EA2F26300D285264F11B0C8301D0207FEB1E2C984445
C899B0ACEBAA74EF014DD1D4BDDB43202C08D2FF9692D8D788478DEC829EB52AFB5AE068FBDBAC49
9A27FACECC391E75C936D55F07BB45EE184DAB45808E15722502F279F89B38C1CB292557E5063597F52C7
5D61001EDC33F4739353E33E56AD273B067C1A2760208529EA421774A5FFFCB3423B1E0051E7702A55D80
CBF2141569F18F87BFF538A1DA8EDBB2693A539F68E0D62D77743F89EACF3B1723BDB25CE2F333FA63C
ACF0E67DF1A431893BB9B352FCB":16:"9A66CF76572A71A17475794FA1C8C70D987E581E990D772BB27C
77C53FF1ECBB31260E9EDAFAEBC79991807E48918EAB8C3A5F03A600F30C69511546AE788EDF53168E2
D035D300EDCD5E4BF3AA2A6D603EA0A7BD11E1C1089657306DF8A64E7F1BC6B266B825C1A6C5F0FC85
775F4CF7ACD63367E42EAFE46511D58AD6DFE0F":16:"844DBDD20925D9164F9A1E2F707076C261CCA833
7D0241392B38AE3C12342F3AC14F8FD6DF4A1C36839662BD0D227344CD55A32AE5DBD2309A9A2B8A2C
82BE6DDDDCE81D1B694775D9047AA765CA0C6E1BB8E61C8B7BE27ED711E8EE2FEAD87F3491F76A6D2
262C14189EACDFD4CEFE0BF9D0A5B49857E0ED22CBEB98DC8D45B":16:"4951A7B174DF972C37BADCC
38457B5EDD1F078BC613E75CE25E08814E12461C7A1C189A70EB8138294298D141244C7A9DE31AB4F6D3
8B40B04D6353CD30F77ADBF66BBDE41C7BE463C5E30AAA3F7BAD6CEE99506DEAAFA2F335C1B1C5C8
8B8ABB0D0387EE0D1B4E7027F7F085A025CEDB5CCE18B88C0462F1C3C910D47C0D4AB":MBEDTLS_ER
R_RSA_KEY_CHECK_FAILED

RSA

Check Public-Private key #3 (Private no N)

rsa_check_pubpriv:2048:16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba222
4703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681

f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4e
cf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4
715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d
755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"3":16:"e79a373182bfaa722eb035f772ad2a94
64bd842de59432c18bbab3a7dfeae318c9b915ee487861ab665a40bd6cda560152578e8579016c929df99fea05b4d64ef
ca1d543850bc8164b40d71ed7f3fa4105df0fb9b9ad2a18ce182c8a4f4f975bea9aa0b9a1438a27a28e97ac8330ef37383
414d1bd64607d6979ac050424fd17":16:"c6749cbb0db8c5a177672d4728a8b22392b2fc4d3b8361d5c0d5055a1b4e4
6d821f757c24eef2a51c561941b93b3ace7340074c058c9bb48e7e7414f42c41da4cccb5c2ba91deb30c586b7fb18af12
a52995592ad139d3be429add6547e044becedaf31fa3b39421e24ee034fbf367d11f6b8f88ee483d163b431e1654ad3e8
9":16:"":16:"3":16:"77B1D99300D6A54E864962DA09AE10CF19A7FB888456BC2672B72AEA52B204914493D
16C184AD201EC3F762E1FBD8702BA796EF953D9EA2F26300D285264F11B0C8301D0207FEB1E2C984445C8
99B0ACEBAA74EF014DD1D4BDDB43202C08D2FF9692D8D788478DEC829EB52AFB5AE068FBDBAC499A
27FACECC391E75C936D55F07BB45EE184DAB45808E15722502F279F89B38C1CB292557E5063597F52C75D
61001EDC33F4739353E33E56AD273B067C1A2760208529EA421774A5FFFCB3423B1E0051E7702A55D80CB
F2141569F18F87BFF538A1DA8EDBB2693A539F68E0D62D77743F89EACF3B1723BDB25CE2F333FA63CAC
F0E67DF1A431893BB9B352FCB":16:"9A66CF76572A71A17475794FA1C8C70D987E581E990D772BB27C77C
53FF1ECBB31260E9EDAFAEBC79991807E48918EAB8C3A5F03A600F30C69511546AE788EDF53168E2D035
D300EDCD5E4BF3AA2A6D603EA0A7BD11E1C1089657306DF8A64E7F1BC6B266B825C1A6C5F0FC85775F
4CF7ACD63367E42EAFE46511D58AD6DFE0F":16:"844DBDD20925D9164F9A1E2F707076C261CCA8337D0
241392B38AE3C12342F3AC14F8FD6DF4A1C36839662BD0D227344CD55A32AE5DBD2309A9A2B8A2C82B
E6DDDDCE81D1B694775D9047AA765CA0C6E1BB8E61C8B7BE27ED711E8EE2FEAD87F3491F76A6D2262
C14189EACDFD4CEFE0BF9D0A5B49857E0ED22CBEB98DC8D45B":16:"4951A7B174DF972C37BADCC384
57B5EDD1F078BC613E75CE25E08814E12461C7A1C189A70EB8138294298D141244C7A9DE31AB4F6D38B4
0B04D6353CD30F77ADBF66BBDE41C7BE463C5E30AAA3F7BAD6CEE99506DEAAFA2F335C1B1C5C88B8
ABB0D0387EE0D1B4E7027F7F085A025CEDB5CCE18B88C0462F1C3C910D47C0D4AB":MBEDTLS_ERR_R
SA_KEY_CHECK_FAILED

RSA

Check Public-Private key #4 (N mismatch)

rsa_check_pubpriv:2048:16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba222
4703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681
f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4e
cf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4
715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d
755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034e":16:"3":16:"e79a373182bfaa722eb035f772ad2a94
64bd842de59432c18bbab3a7dfeae318c9b915ee487861ab665a40bd6cda560152578e8579016c929df99fea05b4d64ef
ca1d543850bc8164b40d71ed7f3fa4105df0fb9b9ad2a18ce182c8a4f4f975bea9aa0b9a1438a27a28e97ac8330ef37383
414d1bd64607d6979ac050424fd17":16:"c6749cbb0db8c5a177672d4728a8b22392b2fc4d3b8361d5c0d5055a1b4e4
6d821f757c24eef2a51c561941b93b3ace7340074c058c9bb48e7e7414f42c41da4cccb5c2ba91deb30c586b7fb18af12
a52995592ad139d3be429add6547e044becedaf31fa3b39421e24ee034fbf367d11f6b8f88ee483d163b431e1654ad3e8
9":16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9
c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d
3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da4
86eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829
c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78
c3d64f35549141486c3b0961a7b4c1a2034f":16:"3":16:"77B1D99300D6A54E864962DA09AE10CF19A7FB88845
6BC2672B72AEA52B204914493D16C184AD201EC3F762E1FBD8702BA796EF953D9EA2F26300D285264F11
B0C8301D0207FEB1E2C984445C899B0ACEBAA74EF014DD1D4BDDB43202C08D2FF9692D8D788478DEC8

29EB52AFB5AE068FBDBAC499A27FACECC391E75C936D55F07BB45EE184DAB45808E15722502F279F89B
38C1CB292557E5063597F52C75D61001EDC33F4739353E33E56AD273B067C1A2760208529EA421774A5FFF
CB3423B1E0051E7702A55D80CBF2141569F18F87BFF538A1DA8EDBB2693A539F68E0D62D77743F89EACF
3B1723BDB25CE2F333FA63CACF0E67DF1A431893BB9B352FCB":16:"9A66CF76572A71A17475794FA1C8
C70D987E581E990D772BB27C77C53FF1ECBB31260E9EDAFAEBC79991807E48918EAB8C3A5F03A600F30
C69511546AE788EDF53168E2D035D300EDCD5E4BF3AA2A6D603EA0A7BD11E1C1089657306DF8A64E7F1
BC6B266B825C1A6C5F0FC85775F4CF7ACD63367E42EAFE46511D58AD6DFE0F":16:"844DBDD20925D916
4F9A1E2F707076C261CCA8337D0241392B38AE3C12342F3AC14F8FD6DF4A1C36839662BD0D227344CD55
A32AE5DBD2309A9A2B8A2C82BE6DDDDCE81D1B694775D9047AA765CA0C6E1BB8E61C8B7BE27ED711
E8EE2FEAD87F3491F76A6D2262C14189EACDFD4CEFE0BF9D0A5B49857E0ED22CBEB98DC8D45B":16:"4
951A7B174DF972C37BADCC38457B5EDD1F078BC613E75CE25E08814E12461C7A1C189A70EB8138294298
D141244C7A9DE31AB4F6D38B40B04D6353CD30F77ADBF66BBDE41C7BE463C5E30AAA3F7BAD6CEE99
506DEAAFA2F335C1B1C5C88B8ABB0D0387EE0D1B4E7027F7F085A025CEDB5CCE18B88C0462F1C3C910
D47C0D4AB":MBEDTLS_ERR_RSA_KEY_CHECK_FAILED

RSA
Check Public-Private key #5 (E mismatch)
rsa_check_pubpriv:2048:16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba222
4703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681
f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4e
cf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4
715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d
755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"17":16:"e79a373182bfaa722eb035f772ad2a9
464bd842de59432c18bbab3a7dfeae318c9b915ee487861ab665a40bd6cda560152578e8579016c929df99fea05b4d64
efca1d543850bc8164b40d71ed7f3fa4105df0fb9b9ad2a18ce182c8a4f4f975bea9aa0b9a1438a27a28e97ac8330ef373
83414d1bd64607d6979ac050424fd17":16:"c6749cbb0db8c5a177672d4728a8b22392b2fc4d3b8361d5c0d5055a1b4
e46d821f757c24eef2a51c561941b93b3ace7340074c058c9bb48e7e7414f42c41da4cccb5c2ba91deb30c586b7fb18af
12a52995592ad139d3be429add6547e044becedaf31fa3b39421e24ee034fbf367d11f6b8f88ee483d163b431e1654ad3
e89":16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452
f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420
d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da
486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c9482
9c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a7
8c3d64f35549141486c3b0961a7b4c1a2034f":16:"3":16:"77B1D99300D6A54E864962DA09AE10CF19A7FB8884
56BC2672B72AEA52B204914493D16C184AD201EC3F762E1FBD8702BA796EF953D9EA2F26300D285264F1
1B0C8301D0207FEB1E2C984445C899B0ACEBAA74EF014DD1D4BDDB43202C08D2FF9692D8D788478DEC
829EB52AFB5AE068FBDBAC499A27FACECC391E75C936D55F07BB45EE184DAB45808E15722502F279F89
B38C1CB292557E5063597F52C75D61001EDC33F4739353E33E56AD273B067C1A2760208529EA421774A5FF
FCB3423B1E0051E7702A55D80CBF2141569F18F87BFF538A1DA8EDBB2693A539F68E0D62D77743F89EAC
F3B1723BDB25CE2F333FA63CACF0E67DF1A431893BB9B352FCB":16:"9A66CF76572A71A17475794FA1C8
C70D987E581E990D772BB27C77C53FF1ECBB31260E9EDAFAEBC79991807E48918EAB8C3A5F03A600F30
C69511546AE788EDF53168E2D035D300EDCD5E4BF3AA2A6D603EA0A7BD11E1C1089657306DF8A64E7F1
BC6B266B825C1A6C5F0FC85775F4CF7ACD63367E42EAFE46511D58AD6DFE0F":16:"844DBDD20925D916
4F9A1E2F707076C261CCA8337D0241392B38AE3C12342F3AC14F8FD6DF4A1C36839662BD0D227344CD55
A32AE5DBD2309A9A2B8A2C82BE6DDDDCE81D1B694775D9047AA765CA0C6E1BB8E61C8B7BE27ED711
E8EE2FEAD87F3491F76A6D2262C14189EACDFD4CEFE0BF9D0A5B49857E0ED22CBEB98DC8D45B":16:"4
951A7B174DF972C37BADCC38457B5EDD1F078BC613E75CE25E08814E12461C7A1C189A70EB8138294298
D141244C7A9DE31AB4F6D38B40B04D6353CD30F77ADBF66BBDE41C7BE463C5E30AAA3F7BAD6CEE99

506DEAAFA2F335C1B1C5C88B8ABB0D0387EE0D1B4E7027F7F085A025CEDB5CCE18B88C0462F1C3C910D47C0D4AB":MBEDTLS_ERR_RSA_KEY_CHECK_FAILED

RSA
Private (Correct)
mbedtls_rsa_private:"59779fd2a39e56640c4fc1e67b60aeffcecd78aed7ad2bdfa464e93d04198d48466b8da7445f25bfa19db2844edd5c8f539cf772cc132b483169d390db28a43bc4ee0f038f6568ffc87447746cb72fefac2d6d90ee3143a915ac4688028805905a68eb8f8a96674b093c495eddd8704461eaa2b345efbb2ad6930acd8023f870":2048:16:"e79a373182bfaa722eb035f772ad2a9464bd842de59432c18bbab3a7dfeae318c9b915ee487861ab665a40bd6cda560152578e8579016c929df99fea05b4d64efca1d543850bc8164b40d71ed7f3fa4105df0fb9b9ad2a18ce182c8a4f4f975bea9aa0b9a1438a27a28e97ac8330ef37383414d1bd64607d6979ac050424fd17":16:"c6749cbb0db8c5a177672d4728a8b22392b2fc4d3b8361d5c0d5055a1b4e46d821f757c24eef2a51c561941b93b3ace7340074c058c9bb48e7e7414f42c41da4cccb5c2ba91deb30c586b7fb18af12a52995592ad139d3be429add6547e044becedaf31fa3b39421e24ee034fbf367d11f6b8f88ee483d163b431e1654ad3e89":16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"3":"48ce62658d82be10737bd5d3579aed15bc82617e6758ba862eeb12d049d7bacaf2f62fce8bf6e980763d1951f7f0eae3a493df9890d249314b39d00d6ef791de0daebf2c50f46e54aeb63a89113defe85de6dbe77642aae9f2eceb420f3a47a56355396e728917f17876bb829fabcaeef8bf7ef6de2ff9e84e6108ea2e52bbb62b7b288efa0a3835175b8b08fac56f7396eceb1c692d419ecb79d80aef5bc08a75d89de9f2b2d411d881c0e3ffad24c311a19029d210d3d3534f1b626f982ea322b4d1cfba476860ef20d4f672f38c371084b5301b429b747ea051a619e4430e0dac33c12f9ee41ca4d81a4f6da3e495aa8524574bdc60d290dd1f7a62e90a67":0

RSA
Private (Data larger than N)
mbedtls_rsa_private:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":2048:16:"e79a373182bfaa722eb035f772ad2a9464bd842de59432c18bbab3a7dfeae318c9b915ee487861ab665a40bd6cda560152578e8579016c929df99fea05b4d64efca1d543850bc8164b40d71ed7f3fa4105df0fb9b9ad2a18ce182c8a4f4f975bea9aa0b9a1438a27a28e97ac8330ef37383414d1bd64607d6979ac050424fd17":16:"c6749cbb0db8c5a177672d4728a8b22392b2fc4d3b8361d5c0d5055a1b4e46d821f757c24eef2a51c561941b93b3ace7340074c058c9bb48e7e7414f42c41da4cccb5c2ba91deb30c586b7fb18af12a52995592ad139d3be429add6547e044becedaf31fa3b39421e24ee034fbf367d11f6b8f88ee483d163b431e1654ad3e89":16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"3":"605baf947c0de49e4f6a0dfb94a43ae318d5df8ed20ba4ba5a37a73fb009c5c9e5cce8b70a25b1c7580f389f0d7092485cdfa02208b70d33482edf07a7eafebdc54862ca0e0396a5a7d09991b9753eb1ffb6091971bb5789c6b121abbcd0a3cbaa39969fa7c28146fce96c6d03272e3793e5be8f5abfa9afcbebb986d7b3050604a2af4d3a40fa6c003781a539a60259d1e84f13322da9e538a49c369b83e7286bf7d30b64bbb773506705da5d5d5483a563a1ffacc902fb75c9a751b1e83cdc7a6db0470056883f48b5a5446b43b1d180ea12ba11a6a8d93b3b32a30156b6084b7f

b142998a2a0d28014b84098ece7d9d5e4d55cc342ca26f5a0167a679dec8":MBEDTLS_ERR_RSA_PRIVATE_FAIL
ED
+ MBEDTLS_ERR_MPI_BAD_INPUT_DATA

RSA Public (Correct)
mbedtls_rsa_public:"59779fd2a39e56640c4fc1e67b60aeffcecd78aed7ad2bdfa464e93d04198d48466b8da7445f25bf
a19db2844edd5c8f539cf772cc132b483169d390db28a43bc4ee0f038f6568ffc87447746cb72fefac2d6d90ee3143a915
ac4688028805905a68eb8f8a96674b093c495eddd8704461eaa2b345efbb2ad6930acd8023f870":2048:16:"b38ac65c8
141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fd
c6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6
b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d5
4c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0a
dab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f355491414
86c3b0961a7b4c1a2034f":16:"3":"1f5e927c13ff231090b0f18c8c3526428ed0f4a7561457ee5afe4d22d5d9220c34ef5
b9a34d0c07f7248a1f3d57f95d10f7936b3063e40660b3a7ca3e73608b013f85a6e778ac7c60d576e9d9c0c5a79ad84ce
ea74e4722eb3553bdb0c2d7783dac050520cb27ca73478b509873cb0dcbd1d51dd8fccb96c29ad314f36d67cc57835d9
2d94defa0399feb095fd41b9f0b2be10f6041079ed4290040449f8a79aba50b0a1f8cf83c9fb8772b0686ec1b29cb1814b
b06f9c024857db54d395a8da9a2c6f9f53b94bec612a0cb306a3eaa9fc80992e85d9d232e37a50cabe48c9343f039601ff
7d95d60025e582aec475d031888310e8ec3833b394a5cf0599101e":0

RSA
Public (Data larger than N)
mbedtls_rsa_public:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b0
2e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1
cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6
ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b8
13d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d7552227
93146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":2048:16:"b38ac65c8141f7f5c96e14470e851936a67bf94cc
6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b9769a892c482b83
0bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509d79c9826e673
bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab203b35255765
261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d7b1458b97da
ed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034f":16:"3":"60
5baf947c0de49e4f6a0dfb94a43ae318d5df8ed20ba4ba5a37a73fb009c5c9e5cce8b70a25b1c7580f389f0d7092485cdf
a02208b70d33482edf07a7eafebdc54862ca0e0396a5a7d09991b9753eb1ffb6091971bb5789c6b121abbcd0a3cbaa399
69fa7c28146fce96c6d03272e3793e5be8f5abfa9afcbebb986d7b3050604a2af4d3a40fa6c003781a539a60259d1e84f1
3322da9e538a49c369b83e7286bf7d30b64bbb773506705da5d5d5483a563a1ffacc902fb75c9a751b1e83cdc7a6db04
70056883f48b5a5446b43b1d180ea12ba11a6a8d93b3b32a30156b6084b7fb142998a2a0d28014b84098ece7d9d5e4d
55cc342ca26f5a0167a679dec8":MBEDTLS_ERR_RSA_PUBLIC_FAILED
+ MBEDTLS_ERR_MPI_BAD_INPUT_DATA

RSA Generate Key - 128bit key
mbedtls_rsa_gen_key:128:3:0

RSA Generate Key (Number of bits too small)
mbedtls_rsa_gen_key:127:3:MBEDTLS_ERR_RSA_BAD_INPUT_DATA

RSA Generate Key (Exponent too small)

mbedtls_rsa_gen_key:128:2:MBEDTLS_ERR_RSA_BAD_INPUT_DATA

RSA Generate Key - 1024 bit key
mbedtls_rsa_gen_key:1024:3:0

RSA Generate Key - 2048 bit key
mbedtls_rsa_gen_key:2048:3:0

RSA Generate Key - 1025 bit key
mbedtls_rsa_gen_key:1025:3:MBEDTLS_ERR_RSA_BAD_INPUT_DATA

RSA PKCS1 Encrypt Bad RNG
depends_on:MBEDTLS_PKCS1_V15
rsa_pkcs1_encrypt_bad_rng:"4E636AF98E40F3ADCFCCB698F4E80B9F":MBEDTLS_RSA_PKCS_V15:2048:16
:"b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a84
17b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61
dc45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec5
9559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c22954
3d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f
35549141486c3b0961a7b4c1a2034f":16:"3":"a42eda41e56235e666e7faaa77100197f657288a1bf183e4820f0c37ce2
c456b960278d6003e0bbcd4be4a969f8e8fd9231e1f492414f00ed09844994c86ec32db7cde3bec7f0c3dbf6ae55baeb2
712fa609f5fc3207a824eb3dace31849cd6a6084318523912bccb84cf42e3c6d6d1685131d69bb545acec827d2b0dfdd5
568b7dcc4f5a11d6916583fefa689d367f8c9e1d95dcd2240895a9470b0c1730f97cd6e8546860bd254801769f54be96e
16362ddcbf34d56035028890199e0f48db38642cb66a4181e028a6443a404fea284ce02b4614b683367d40874e50561
1d23142d49f06feea831d52d347b13610b413c4efc43a6de9f0b08d2a951dc503b6":MBEDTLS_ERR_RSA_RNG_F
AILED

RSA
Selftest
depends_on:MBEDTLS_SELF_TEST
rsa_selftest:
-----BEGIN X509 CRL-----
MIICejCCATECAQEwPgYJKoZIhvcNAQEKMDGgDTALBglghkgBZQMEAgShGjAYBgkq
hkiG9w0BAQgwCwYJYIZIAWUDBAIEogQCAgDiMDsxCzAJBgNVBAYTAk5MMREwDwYD
VQQKEwhQb2xhclNTTDEZMBcGA1UEAxMQUG9sYXJTU0wgVGVzdCBDQRcNMTQwMTIw
MTM1NjA2WhcNMjQwMTE4MTM1NjA2WjAoMBICAQoXDTEzMDkyNDE2MjgzOFowEgIB
FhcNMTQwMTIwMTM0MzA1WqBnMGUwYwYDVR0jBFwwWoAUtFrkpbPe0lL2udWmlQ/r
PrzH/f+hP6Q9MDsxCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEZMBcG
A1UEAxMQUG9sYXJTU0wgVGVzdCBDQYIBADA+BgkqhkiG9w0BAQowMaANMAsGCWCG
SAFlAwQCBKEaMBgGCSqGSIb3DQEBCDALBglghkgBZQMEAgSiBAICAOIDggEBAEJI
i9sQOzMvvOTksN48+X+kk/wkLMKRGI222lqU6y6tP1LX3OE/+KN8gPXR+lCC+e0v
TsRTJkpKEcmHZoP/8kOtZnLb9PdITKGMQnZ+dmn5MFEzZI/zyrYWuJTuK1Q83w0e
Mc88cAhu8i4PTk/WnsWDphK1Q2YRupmmwWSUpp1Z2rpR+YSCedC01TVrtSUJUBw9
NSqKDhyWYJIbS6/bFaERswC8xlMRhyLHUvikjmAK36TbIdhTnEffHOPW75sEOEEB
f0A3VtlZ7y5yt2/a6vOauJCivxKt/PutdHfBqH43QQmoVLWC2FmT9ADTJwcsZB3D
a6JSqCIMRCQY2JOUn0A=
-----END X509 CRL-----

-----BEGIN CERTIFICATE-----
MIIDhzCCAm+gAwIBAgIBADANBgkqhkiG9w0BAQsFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UECgwIUG9sYXJTU0wxGTAXBgNVBAMMEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTcwNTA0MTY1NzAxWhcNMjcwNTA1MTY1NzAxWjA7MQswCQYDVQQGEwJOTDERMA8G
A1UECgwIUG9sYXJTU0wxGTAXBgNVBAMMEFBvbGFyU1NMIFRlc3QgQ0EwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDA3zf8F7vglp0/ht6WMn1EpRagzSHx
mdTs6st8GFgIlKXsm8WL3xoemTiZhx57wI053zhdcHgH057Zk+i5clHFzqMwUqny
50BwFMtEonILwuVA+T7lpg6z+exKY8C4KQB0nFc7qKUEkHHxvYPZP9al4jwqj+8n
YMPGn8u67GB9t+aEMr5P+1gmIgNb1LTV+/Xjli5wwOQuvfwu7uJBVcA0Ln0kcmnL
R7EUQIN9Z/SG9jGr8XmksrUuEvmEF/Bibyc+E1ixVA0hmnM3oTDPb5Lc9un8rNsu
KNF+AksjoBXyOGVkCeoMbo4bF6BxyLObyavpw/LPh5aPgAIynplYb6LVAgMBAAGj
gZUwgZIwHQYDVR0OBBYEFLRa5KWz3tJS9rnVppUP6z68x/3/MGMGA1UdIwRcMFqA
FLRa5KWz3tJS9rnVppUP6z68x/3/oT+kPTA7MQswCQYDVQQGEwJOTDERMA8GA1UE
CgwIUG9sYXJTU0wxGTAXBgNVBAMMEFBvbGFyU1NMIFRlc3QgQ0GCAQAwDAYDVR0T
BAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAQEAHK/HHrTZMnnVMpde1io+voAtql7j
4sRhLrjD7o3THtwRbDa2diCvpq0Sq23Ng2LMYoXsOxoL/RQK3iN7UKxV3MKPEr0w
XQS+kKQqiT2bsfrjnWMVHZtUOMpm6FNqcdGm/Rss3vKda2lcKl8kUnq/ylc1+QbB
G6A6tUvQcr2ZyWfVg+mM5XkhTrOOXus2OLikb4WwEtJTJRNE0f+yPODSUz0/vT57
ApH0CnB80bYJshYHPHHymOtleAB8KSYtqm75g/YNobjnjB6cm4HkW3OZRVIl6fYY
n20NRVA1Vjs6GAROr4NqW4k/+LofY9y0LLDE+p0oIEKXIsIvhPr39swxSA==
-----END
 CERTIFICATE-----
0 #J#XB00,*H=!/0!yf~Ub-(Y[!H;^6AA$"@PKnqwp[WF?F5
 +
-----BEGIN CERTIFICATE-----
MIICLDCCAbKgAwIBAgIBDTAKBggqhkjOPQQDAjA+MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EwHhcN
MTMwOTI0MTU1MjA0WhcNMjMwOTIyMTU1MjA0WjBBMQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxHzAdBgNVBAMTFlBvbGFyU1NMIFRlc3QgQ2xpZW50IDIw
WTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAARX5a6xc9/TrLuTuIH/Eq7u5lOszlVT
9jQOzC7jYyUL35ji81xgNpbA1RgUcOV/n9VLRRjlsGzVXPiWj4dwo+THo4GdMIGa
MAkGA1UdEwQCMAAwHQYDVR0OBBYEFHoAX4Zk/OBd5REQO7LmO8QmP8/iMG4GA1Ud
IwRnMGWAFJ1tICRJAT8ry3i1Gbx+JMnb+zZ8oUKkQDA+MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0GC
CQDBQ+J+YkPM6DAKBggqhkjOPQQDAgNoADBlAjBKZQ17IIOimbmoD/yN7o89u3BM
lgOsjnhw3fIOoLIWy2WOGsk/LGF++DzvrRzuNiACMQCd8iem1XS4JK7haj8xocpU
LwjQje5PDGHfd3h9tP38Qknu5bJqws0md2KOKHyeV0U=
-----END CERTIFICATE-----
Notes:
* Pull requests cannot be accepted until:
- The submitter has [accepted the online agreement here with a click
through](https://developer.mbed.org/contributor_agreement/)
  or for companies or those that do not wish to create an mbed account, a slightly different agreement can be found
[here](https://www.mbed.com/en/about-mbed/contributor-license-agreements/)
- The PR follows the [mbed TLS coding standards](https://tls.mbed.org/kb/development/mbedtls-coding-standards)
* This is just a template, so feel free to use/remove the unnecessary things
Description
A few sentences describing the overall goals of the pull request's commits.

Status
READY/IN DEVELOPMENT/HOLD

Requires Backporting
When there is a bug fix, it should be backported to all maintained and supported branches.
Changes do not have to be backported if:
- This PR is a new feature\enhancement
- This PR contains changes in the API. If this is true, and there is a need for the fix to be backported, the fix should be handled differently in the legacy branch

Yes | NO
Which branch?

Migrations
If there is any API change, what's the incentive and logic for it.

YES | NO

Additional comments
Any additional information that could be of interest

Todos
- [ ] Tests
- [ ] Documentation
- [ ] Changelog updated
- [ ] Backported

Steps to test or reproduce
Outline the steps to test or reproduce the PR here.
add_executable(aescrypt2 aescrypt2.c)
target_link_libraries(aescrypt2 mbedtls)

add_executable(crypt_and_hash crypt_and_hash.c)
target_link_libraries(crypt_and_hash mbedtls)

install(TARGETS aescrypt2 crypt_and_hash
    DESTINATION "bin"
    PERMISSIONS OWNER_READ OWNER_WRITE OWNER_EXECUTE GROUP_READ GROUP_EXECUTE WORLD_READ WORLD_EXECUTE)
-----BEGIN EC PRIVATE KEY-----
MF8CAQEEGItTogpE7AOnjvYuTqm+9OabmsX02XKIAqAKBggqhkjOPQMBAaE0AzIA
BH0AoQyUhPABS38y67uEVs4O3RXmKKrBdUR7/L2QPB8EC2p5fQcsej6EFasvlTdJ
/w==
-----END EC PRIVATE KEY-----

```
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
   <Configuration>Release</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\random\gen_random_havege.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">
   <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid>{71257802-BBCA-99F5-E9D2-905738F30893}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>gen_random_havege</RootNamespace>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'"
 Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
```

```
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')"
 Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup
 Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
```

```
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
   <PrecompiledHeader>
   </PrecompiledHeader>
   <WarningLevel>Level3</WarningLevel>
   <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
   <SubSystem>Console</SubSystem>
   <GenerateDebugInformation>true</GenerateDebugInformation>
   <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
   <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
   <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
   <PrecompiledHeader>
   </PrecompiledHeader>
   <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
   <SubSystem>Console</SubSystem>
   <GenerateDebugInformation>true</GenerateDebugInformation>
   <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
   <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
   <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
```

```
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
  </Link>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
  <Import Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTAwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
```

DTALBgNVBAMMBENBMTEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATZwR+WK6NB
F/7riFdN63c8hjYddZRR4lrzVNPwiBQxnnxwpPyrD9A6aPPmLc6SqGOJW4ZGVCco
IBze9RJVeiB9o4GJMIGGMB0GA1UdDgQWBBSOSt6ePyMRT6PGMaIi7FqNX9MKtDBX
BgNVHSMEUDBOgBQtxZSLJAkEz+2RKMQexM6EtsfgcqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA5ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgN//NqM0FrkrMjmxoeCY9DgxkH2R6sQ4d
NgtwCZAIqEICIBs4vupaVcuvni9tltbP26wi7c0FR+blZuo5DPIA3SVe
-----END CERTIFICATE-----
SHA-1 Test Vector NIST CAVS #1
depends_on:MBEDTLS_SHA1_C
mbedtls_sha1:"":"da39a3ee5e6b4b0d3255bfef95601890afd80709"

SHA-1 Test Vector NIST CAVS #2
depends_on:MBEDTLS_SHA1_C
mbedtls_sha1:"a8":"99f2aa95e36f95c2acb0eaf23998f030638f3f15"

SHA-1 Test Vector NIST CAVS #3
depends_on:MBEDTLS_SHA1_C
mbedtls_sha1:"3000":"f944dcd635f9801f7ac90a407fbc479964dec024"

SHA-1 Test Vector NIST CAVS #4
depends_on:MBEDTLS_SHA1_C
mbedtls_sha1:"42749e":"a444319e9b6cc1e8464c511ec0969c37d6bb2619"

SHA-1 Test Vector NIST CAVS #5
depends_on:MBEDTLS_SHA1_C
mbedtls_sha1:"9fc3fe08":"16a0ff84fcc156fd5d3ca3a744f20a232d172253"

SHA-1 Test Vector NIST CAVS #6
depends_on:MBEDTLS_SHA1_C
mbedtls_sha1:"b5c1c6f1af":"fec9deebfcdedaf66dda525e1be43597a73a1f93"

SHA-1 Test Vector NIST CAVS #7
depends_on:MBEDTLS_SHA1_C
mbedtls_sha1:"ec29561244ede706b6eb30a1c371d74450a105c3f9735f7fa9fe38cf67f304a5736a106e92e17139a6813
b1c81a4f3d3fb9546ab4296fa9f722826c066869edacd73b2548035185813e22634a9da44000d95a281ff9f264ecce0a9
31222162d021cca28db5f3c2aa24945ab1e31cb413ae29810fd794cad5dfaf29ec43cb38d198fe4ae1da2359780221405
bd6712a5305da4b1b737fce7cd21c0eb7728d08235a9011":"970111c4e77bcc88cc20459c02b69b4aa8f58217"

SHA-1
Test Vector NIST CAVS #8
depends_on:MBEDTLS_SHA1_C
mbedtls_sha1:"5fc2c3f6a7e79dc94be526e5166a238899d54927ce470018fbfd668fd9dd97cbf64e2c91584d01da63be
3cc9fdff8adfefc3ac728e1e335b9cdc87f069172e323d094b47fa1e652afe4d6aa147a9f46fda33cacb65f3aa12234746b9
007a8c85fe982afed7815221e43dba553d8fe8a022cdac1b99eeeea359e5a9d2e72e382dffa6d19f359f4f27dc3434cd27
daeeda8e38594873398678065fbb23665aba9309d946135da0e4a4afdadff14db18e85e71dd93c3bf9faf7f25c8194c426
9b1ee3d9934097ab990025d9c3aaf63d5109f52335dd3959d38ae485050e4bbb6235574fc0102be8f7a306d6e8de6ba6
becf80f37415b57f9898a5824e77414197422be3d36a6080":"0423dc76a8791107d14e13f5265b343f24cc0f19"

SHA-1 Test Vector NIST CAVS #9
depends_on:MBEDTLS_SHA1_C
mbedtls_sha1:"0f865f46a8f3aed2da18482aa09a8f390dc9da07d51d1bd10fe0bf5f3928d5927d08733d32075535a6d1c8ac1b2dc6ba0f2f633dc1af68e3f0fa3d85e6c60cb7b56c239dc1519a007ea536a07b518ecca02a6c31b46b76f021620ef3fc6976804018380e5ab9c558ebfc5cb1c9ed2d974722bf8ab6398f1f2b82fa5083f85c16a5767a3a07271d67743f00850ce8ec428c7f22f1cf01f99895c0c844845b06a06cecb0c6cf83eb55a1d4ebc44c2c13f6f7aa5e0e08abfd84e7864279057abc471ee4a45dbbb5774afa24e51791a0eada11093b88681fe30baa3b2e94113dc63342c51ca5d1a6096d0897b626e42cb91761058008f746f35465465540ad8c6b8b60f7e1461b3ce9e6529625984cb8c7d46f07f735be067588a0117f23e34ff57800e2bbe9a1605fde6087fb15d22c5d3ac47566b8c448b0cee40373e5ba6eaa21abee71366afbb27dbbd300477d70c371e7b8963812f5ed4fb784fb2f3bd1d3afe883cdd47ef32beaea":"6692a71d73e00f27df976bc56df4970650d90e45"

SHA-1
Test Vector NIST CAVS #10
depends_on:MBEDTLS_SHA1_C
mbedtls_sha1:"8236153781bd2f1b81ffe0def1beb46f5a70191142926651503f1b3bb1016acdb9e7f7acced8dd168226f118ff664a01a8800116fd023587bfba52a2558393476f5fc69ce9c65001f23e70476d2cc81c97ea19caeb194e224339bcb23f77a83feac5096f9b3090c51a6ee6d204b735aa71d7e996d380b80822e4dfd43683af9c7442498cacbea64842dfda238cb099927c6efae07fdf7b23a4e4456e0152b24853fe0d5de4179974b2b9d4a1cdbefcbc01d8d311b5dda059136176ea698ab82acf20dd490be47130b1235cb48f8a6710473cfc923e222d94b582f9ae36d4ca2a32d141b8e8cc36638845fbc499bce17698c3fecae2572dbbd470552430d7ef30c238c2124478f1f780483839b4fb73d63a9460206824a5b6b65315b21e3c2f24c97ee7c0e78faad3df549c7ca8ef241876d9aafe9a309f6da352bec2caaa92ee8dca392899ba67dfed90aef33d41fc2494b765cb3e2422c8e595dabbfaca217757453fb322a13203f425f6073a9903e2dc5818ee1da737afc345f0057744e3a56e1681c949eb12273a3bfc20699e423b96e44bd1ff62e50a848a890809bfe1611c6787d3d741103308f849a790f9c015098286dbacfc34c1718b2c2b77e32194a75dda37954a320fa68764027852855a7e5b5274eb1e2cbcd27161d98b59ad245822015f48af82a45c0ed59be94f9af03d9736048570d6e3ef63b1770bc98dfb77de84b1bb1708d872b625d9ab9b06c18e5dbbf34399391f0f8aa26ec0dac7ff4cb8ec97b52bcb942fa6db2385dcd1b3b9d567aaeb425d567b0ebe267235651a1ed9bf78fd93d3c1dd077fe340bb04b00529c58f45124b717c168d07e9826e33376988bc5cf62845c2009980a4dfa69fbc7e5a0b1bb20a5958ca967aec68eb31dd8fccca9afcd30a26bab26279f1bf6724ff":"11863b483809ef88413ca9b0084ac4a5390640af"

SHA-224
Test Vector NIST CAVS #1
depends_on:MBEDTLS_SHA256_C
sha224:"":"d14a028c2a3a2bc9476102bb288234c415a2b01f828ea62ac5b3e42f"

SHA-224 Test Vector NIST CAVS #2
depends_on:MBEDTLS_SHA256_C
sha224:"ff":"e33f9d75e6ae1369dbabf81b96b4591ae46bba30b591a6b6c62542b5"

SHA-224 Test Vector NIST CAVS #3
depends_on:MBEDTLS_SHA256_C
sha224:"984c":"2fa9df9157d9e027cfbc4c6a9df32e1adc0cbe2328ec2a63c5ae934e"

SHA-224 Test Vector NIST CAVS #4
depends_on:MBEDTLS_SHA256_C
sha224:"50efd0":"b5a9820413c2bf8211fbbf5df1337043b32fa4eafaf61a0c8e9ccede"

SHA-224 Test Vector NIST CAVS #5
depends_on:MBEDTLS_SHA256_C
sha224:"e5e09924":"fd19e74690d291467ce59f077df311638f1c3a46e510d0e49a67062d"

SHA-224 Test Vector NIST CAVS #6
depends_on:MBEDTLS_SHA256_C
sha224:"21ebecb914":"78f4a71c21c694499ce1c7866611b14ace70d905012c356323c7c713"

SHA-224 Test Vector NIST CAVS #7
depends_on:MBEDTLS_SHA256_C
sha224:"fc488947c1a7a589726b15436b4f3d9556262f98fc6422fc5cdf20f0fad7fe427a3491c86d101ffe6b7514f0626
8f65b2d269b0f69ad9a97847eff1c16a2438775eb7be6847ccf11cb8b2e8dcd6640b095b49c0693fe3cf4a66e2d9b7ad6
8bff14f3ad69abf49d0aba36cbe0535202deb6599a47225ef05beb351335cd7bc0f480d691198c7e71305ffd53b39d332
42bb79cfd98bfd69e137b5d18b2b89ac9ace01c8dbdcf2533cce3682ecc52118de0c1062ec2126c2e657d6ea3d9e2398e
705d4b0b1f1ceecb266dffc4f31bf42744fb1e938dc22a889919ee1e73f463f7871fed720519e32186264b7ef2a0e5d9a1
8e6c95c0781894f77967f048951dec3b4d892a38710b1e3436d3c29088eb8b3da1789c25db3d3bc6c26081206e7155d
210a89b80ca6ea877c41ff9947c0f25625dcb118294a163501f6239c326661a958fd12da4cd15a899f8b88cc723589056
eaec5aa04a4cf5dbb6f480f9660423ccf38c486e210707e0fb25e1f126ceb2616f63e147a647dab0af9ebe89d65458bf636
154a46e4cab95f5ee62da2c7974cd14b90d3e4f99f81733e85b3c1d5da2b508d9b90f5eed7eff0d9c7649de62bee00375
454fee4a39576a5bbfdae428e7f8097bdf7797f167686cb68407e49079e4611ff3402b6384ba7b7e522bd2bb11ce8fd02
ea4c1604d163ac4f6dde50b8b1f593f7edaadeac0868ed97df690200680c25f0f5d85431a529e4f339089dcdeda105e4ee
51dead704cdf5a605c55fb055c9b0e86b8ba1b564c0dea3eb790a595cb103cb292268b07c5e59371e1a7ef597cd4b229
77a820694c9f9aeb55d9de3ef62b75d6e656e3336698d960a3787bf8cf5b926a7faeef52ae128bcb5dc9e66d94b016c7b
8e034879171a2d91c381f57e6a815b63b5ee6a6d2ff435b49f14c963966960194430d78f8f87627a67757fb3532b28955
0894da6dce4817a4e07f4d56877a1102ffcc8befa5c9f8fca6a4574d93ff70376c8861e0f8108cf907fce77ecb49728f86f0
34f80224b9695682e0824462f76cdb1fd1af151337b0d85419047a7aa284791718a4860cd586f7824b95bc837b6fd4f9
be5aade68456e20356aa4d943dac36bf8b67b9e8f9d01a00fcda74b798bafa746c661b010f75b59904b29d0c804150481
1c4065f82cf2ead58d2f595cbd8bc3e7043f4d94577b373b7cfe16a36fe564f505c03b70cfeb5e5f411c79481338aa67e8
6b3f5a2e77c21e454c333ae3da943ab723ab5f4c940395319534a5575f64acba0d0ecc43f60221ed3badf7289c9b3a7b9
03a2d6c94e15fa4c310dc4fa7faa0c24f405160a1002dbef20e4105d481db982f7243f79400a6e4cd9753c4b9732a4757
5f504b20c328fe9add7f432a4f075829da07b53b695037dc51737d3cd731934df333cd1a53fcf65aa31baa450ca501a6fa
e26e322347e618c5a444d92e9fec5a8261ae38b98fee5be77c02cec09ddccd5b3de92036":"1302149d1e197c41813b05
4c942329d420e366530f5517b470e964fe"

SHA-256
Test Vector NIST CAVS #1
depends_on:MBEDTLS_SHA256_C
mbedtls_sha256:"":"e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855"

SHA-256 Test Vector NIST CAVS #2
depends_on:MBEDTLS_SHA256_C
mbedtls_sha256:"bd":"68325720aabd7c82f30f554b313d0570c95accbb7dc4b5aae11204c08ffe732b"

SHA-256 Test Vector NIST CAVS #3
depends_on:MBEDTLS_SHA256_C
mbedtls_sha256:"5fd4":"7c4fbf484498d21b487b9d61de8914b2eadaf2698712936d47c3ada2558f6788"

SHA-256 Test Vector NIST CAVS #4

depends_on:MBEDTLS_SHA256_C
mbedtls_sha256:"b0bd69":"4096804221093ddccfbf46831490ea63e9e99414858f8d75ff7f642c7ca61803"

SHA-256 Test Vector NIST CAVS #5
depends_on:MBEDTLS_SHA256_C
mbedtls_sha256:"c98c8e55":"7abc22c0ae5af26ce93dbb94433a0e0b2e119d014f8e7f65bd56c61ccccd9504"

SHA-256 Test Vector NIST CAVS #6
depends_on:MBEDTLS_SHA256_C
mbedtls_sha256:"81a723d966":"7516fb8bb11350df2bf386bc3c33bd0f52cb4c67c6e4745e0488e62c2aea2605"

SHA-256
Test Vector NIST CAVS #7
depends_on:MBEDTLS_SHA256_C
mbedtls_sha256:"8390cf0be07661cc7669aac54ce09a37733a629d45f5d983ef201f9b2d13800e555d9b1097fec3b783d7a50dcb5e2b644b96a1e9463f177cf34906bf388f366db5c2deee04a30e283f764a97c3b377a034fefc22c259214faa99babaff160ab0aaa7e2ccb0ce09c6b32fe08cbc474694375aba703fadbfa31cf685b30a11c57f3cf4edd321e57d3ae6ebb1133c8260e75b9224fa47a2bb205249add2e2e62f817491482ae152322be0900355cdcc8d42a98f82e961a0dc6f537b7b410eff105f59673bfb787bf042aa071f7af68d944d27371c64160fe9382772372516c230c1f45c0d6b6cca7f274b394da9402d3eafdf733994ec58ab22d71829a98399574d4b5908a447a5a681cb0dd50a31145311d92c22a16de1ead66a5499f2dceb4cae694772ce90762ef8336afec653aa9b1a1c4820b221136dfce80dce2ba920d88a530c9410d0a4e0358a3a11052e58dd73b0b179ef8f56fe3b5a2d117a73a0c38a1392b6938e9782e0d86456ee4884e3c39d4d75813f13633bc79baa07c0d2d555afbf207f52b7dca126d015aa2b9873b3eb065e90b9b065a5373fe1fb1b20d594327d19fba56cb81e7b6696605ffa56eba3c27a438697cc21b201fd7e09f18deea1b3ea2f0d1edc02df0e20396a145412cd6b13c32d2e605641c948b714aec30c0649dc44143511f35ab0fd5dd64c34d06fe86f3836dfe9edeb7f08cfc3bd409568263562421 91f99f53473f32b0cc0cf9321d6c92a112e8db90b86ee9e87cc32d0343db01e32ce9eb782cb24efbbbeb440fe929e8f2bf8dfb1550a3a2e742e8b455a3e5730e9e6a7a9824d17acc0f72a7f67eae0f0970f8bde46dcdefaed3047cf807e7f00a42e5fd11d40f5e98533d7574425b7d2bc3b3845c443008b58980e768e464e17cc6f6b3939eee52f713963d07d8c4abf02448ef0b889c9671e2f8a436ddeeffcca7176e9bf9d1005ecd377f2fa67c23ed1f137e60bf46018a8bd613d038e883704fc26e798969df35ec7bbc6a4fe46d8910bd82fa3cded265d0a3b6d399e4251e4d8233daa21b5812fded6536198ff13aa5a1cd46a5b9a17a4ddc1d9f85544d1d1cc16f3df858038c8e071a11a7e157a85a6a8dc47e88d75e7009a8b26fdb73f33a2a70f1e0c259f8f9533b9b8f9af9288b7274f21baeec78d396f8bacdcc22471207d9b4efccd3fedc5c5a2214ff5e51c553f35e21ae696fe51e8df733a8e06f50f419e599e9f9e4b37ce643fc810faaa47989771509d69a110ac916261427026369a21263ac4460fb4f708f8ae28599856db7cb6a43ac8e03d64a9609807e76c5f312b9d1863bfa304e8953647648b4f4ab0ed995e":"4109cdbec3240ad74cc6c37f39300f70fede16e21efc77f7865998714aad0b5e"

SHA-384
Test Vector NIST CAVS #1
depends_on:MBEDTLS_SHA512_C
sha384:"":"38b060a751ac96384cd9327eb1b1e36a21fdb71114be07434c0cc7bf63f6e1da274edebfe76f65fbd51ad2f14898b95b"

SHA-384 Test Vector NIST CAVS #2
depends_on:MBEDTLS_SHA512_C
sha384:"ab":"fb94d5be118865f6fcbc978b825da82cff188faec2f66cb84b2537d74b4938469854b0ca89e66fa2e182834736629f3d"

SHA-384 Test Vector NIST CAVS #3

depends_on:MBEDTLS_SHA512_C
sha384:"7c27":"3d80be467df86d63abb9ea1d3f9cb39cd19890e7f2c53a6200bedc5006842b35e820dc4e0ca90ca9b97ab23ef07080fc"

SHA-384 Test Vector NIST CAVS #4
depends_on:MBEDTLS_SHA512_C
sha384:"31f5ca":"78d54b943421fdf7ba90a7fb9637c2073aa480454bd841d39ff72f4511fc21fb67797b652c0c823229342873d3bef955"

SHA-384 Test Vector NIST CAVS #5
depends_on:MBEDTLS_SHA512_C
sha384:"7bdee3f8":"8bdafba0777ee446c3431c2d7b1fbb631089f71d2ca417abc1d230e1aba64ec2f1c187474a6f4077d372c14ad407f99a"

SHA-384 Test
Vector NIST CAVS #6
depends_on:MBEDTLS_SHA512_C
sha384:"8f05604915":"504e414bf1db1060f14c8c799e25b1e0c4dcf1504ebbd129998f0ae283e6de86e0d3c7e879c73ec3b1836c3ee89c2649"

SHA-384 Test Vector NIST CAVS #7
depends_on:MBEDTLS_SHA512_C
sha384:"665da6eda214":"4c022f112010908848312f8b8f1072625fd5c105399d562ea1d56130619a7eac8dfc3748fd05ee37e4b690be9daa9980"

SHA-384 Test Vector NIST CAVS #8
depends_on:MBEDTLS_SHA512_C
sha384:"7f46ce506d593c4ed53c82edeb602037e0485befbee03f7f930fe532d18ff2a3f5fd6076672c8145a1bf40dd94f7abab47c9ae71c234213d2ad1069c2dac0b0ba15257ae672b8245960ae55bd50315c0097daa3a318745788d70d14706910809ca6e396237fe4934fa46f9ce782d66606d8bd6b2d283b1160513ce9c24e9f084b97891f99d4cdefc169a029e431ca772ba1bba426fce6f01d8e286014e5acc66b799e4db62bd4783322f8a32ff78e0de3957df50ce10871f4e0680df4e8ca3960af9bc6f4efa8eb3962d18f474eb178c3265cc46b8f2ff5ab1a7449fea297dfcfabfa01f28abbb7289bb354b691b5664ec6d098af51be19947ec5ba7ebd66380d1141953ba78d4aa5401679fa7b0a44db1981f864d3535c45afe4c61183d5b0ad51fae71ca07e34240283959f7530a32c70d95a088e501c230059f333b0670825009e7e22103ef22935830df1fac8ef877f5f3426dd54f7d1128dd871ad9a7d088f94c0e8712013295b8d69ae7623b880978c2d3c6ad26dc478f8dc47f5c0adcc618665dc3dc205a9071b2f2191e16cac5bd89bb59148fc719633752303aa08e518dbc389f0a5482caaa4c507b8729a6f3edd061efb39026cecc6399f51971cf7381d605e144a5928c8c2d1ad7467b05da2f202f4f3234e1aff19a0198a28685721c3d2d52311c721e3fdcbaf30214cdc3acff8c433880e104fb63f2df7ce69a97857819ba7ac00ac8eae1969764fde8f68cf8e0916d7e0c151147d4944f99f42ae50f30e1c79a42d2b6c5188d133d3cbbf69094027b354b295ccd0f7dc5a87d73638bd98ebfb00383ca0fa69cb8dcb35a12510e5e07ad8789047d0b63841a1bb928737e8b0a0c33254f47aa8bfbe3341a09c2b76dbcefa67e30df300d34f7b8465c4f869e51b6bcfe6cf68b238359a645036bf7f63f02924e087ce7457e483b6025a859903cb484574aa3b12cf946f32127d537c33bee3141b5db96d10a148c50ae045f287210757710d6846e04b202f79e87dd9a56bc6da15f84a77a7f63935e1dee00309cd276a8e7176cb04da6bb0e9009534438732cb42d008008853d38d19beba46e61006e30f7efd1bc7c2906b024e4ff898a1b58c448d68b43c6ab63f34f85b3ac6aa4475867e51b583844cb23829f4b30f4bdd817d88e2ef3e7b4fc0a624395b05ec5e8686082b24d29fef2b0d3c29e031d5f94f504b1d3df9361eb5ffbadb242e66c39a8094cfe62f85f639f3fd65fc8ae0c74a8f4c6e1d070b9183a434c722caaa0225f8bcd68614d6f0738ed62f8484ec96077d155c08e26c46be262a73e3551698bd70d8d5610cf37c4c306eed04ba6a040a9c3e6d7e15e8acda17f477c2484cf5c56b813313927be8387b1024f995e98fc87f1029091c01424bdc2b296c2eadb7d25b3e762a2fd0c2dcd1727ddf91db97c59

84305265f3695a7f5472f2d72c94d68c27914f14f82aa8dd5fe4e2348b0ca967a3f98626a091552f5d0ffa2bf10350d23c996256c01fdeffb2c2c612519869f877e4929c6e95ff15040f1485e22ed14119880232fef3b57b3848f15b1766a5552879df8f06":"cba9e3eb12a6f83db11e8a6ff40d1049854ee094416bc527fea931d8585428a8ed6242ce81f6769b36e2123a5c23483e"

SHA-512
Test Vector NIST CAVS #1
depends_on:MBEDTLS_SHA512_C
mbedtls_sha512:"":"cf83e1357eefb8bdf1542850d66d8007d620e4050b5715dc83f4a921d36ce9ce47d0d13c5d85f2b0ff8318d2877eec2f63b931bd47417a81a538327af927da3e"

SHA-512 Test Vector NIST CAVS #2
depends_on:MBEDTLS_SHA512_C
mbedtls_sha512:"8f":"e4cd2d19931b5aad9c920f45f56f6ce34e3d38c6d319a6e11d0588ab8b838576d6ce6d68eea7c830de66e2bd96458bfa7aafbcbec981d4ed040498c3dd95f22a"

SHA-512
Test Vector NIST CAVS #3
depends_on:MBEDTLS_SHA512_C
mbedtls_sha512:"e724":"7dbb520221a70287b23dbcf62bfc1b73136d858e86266732a7fffa875ecaa2c1b8f673b5c065d360c563a7b9539349f5f59bef8c0c593f9587e3cd50bb26a231"

SHA-512 Test Vector NIST CAVS #4
depends_on:MBEDTLS_SHA512_C
mbedtls_sha512:"de4c90":"33ce98281045a5c4c9df0363d8196f1d7dfcd5ee46ac89776fd8a4344c12f123a66788af5bd41ceff1941aa5637654b4064c88c14e00465ab79a2fc6c97e1014"

SHA-512 Test Vector NIST CAVS #5
depends_on:MBEDTLS_SHA512_C
mbedtls_sha512:"a801e94b":"dadb1b5a27f9fece8d86adb2a51879beb1787ff28f4e8ce162cad7fee0f942efcabbf738bc6f797fc7cc79a3a75048cd4c82ca0757a324695bfb19a557e56e2f"

SHA-512 Test Vector NIST CAVS #6
depends_on:MBEDTLS_SHA512_C
mbedtls_sha512:"94390d3502":"b6175c4c4cccf69e0ce5f0312010886ea6b34d43673f942ae42483f9cbb7da817de4e11b5d58e25a3d9bd721a22cdffe1c40411cc45df1911fa5506129b69297"

SHA-512
Test Vector NIST CAVS #7
depends_on:MBEDTLS_SHA512_C
mbedtls_sha512:"49297dd63e5f":"1fcc1e6f6870859d11649f5e5336a9cd16329c029baf04d5a6edf257889a2e9522b497dd656bb402da461307c4ee382e2e89380c8e6e6e7697f1e439f650fa94"

SHA-512 Test Vector NIST CAVS #8
depends_on:MBEDTLS_SHA512_C
mbedtls_sha512:"990d1ae71a62d7bda9bfdaa1762a68d296eee72a4cd946f287a898fbabc002ea941fd8d4d991030b4d27a637cce501a834bb95eab1b7889a3e784c7968e67cbf552006b206b68f76d9191327524fcc251aeb56af483d10b4e0c6c5e599ee8c0fe4faeca8293844a8547c6a9a90d093f2526873a19ad4a5e776794c68c742fb834793d2dfcb7fea46c63af

4b70fd11cb6e41834e72ee40edb067b292a794990c288d5007e73f349fb383af6a756b8301ad6e5e0aa8cd614399bb3a
452376b1575afa6bdaeaafc286cb064bb91edef97c632b6c1113d107fa93a0905098a105043c2f05397f702514439a08a
9e5ddc196100721d45c8fc17d2ed659376f8a00bd5cb9a0860e26d8a29d8d6aaf52de97e9346033d6db501a35dbbaf97
c20b830cd2d18c2532f3a59cc497ee64c0e57d8d060e5069b28d86edf1adcf59144b221ce3ddaef134b3124fbc7dd0002
40eff0f5f5f41e83cd7f5bb37c9ae21953fe302b0f6e8b68fa91c6ab99265c64b2fd9cd4942be04321bb5d6d71932376c6
f2f88e02422ba6a5e2cb765df93fd5dd0728c6abdaf03bce22e0678a544e2c3636f741b6f4447ee58a8fc656b43ef81793
2176adbfc2e04b2c812c273cd6cbfa4098f0be036a34221fa02643f5ee2e0b38135f2a18ecd2f16ebc45f8eb31b8ab967a
1567ee016904188910861ca1fa205c7adaa194b286893ffe2f4fbe0384c2aef72a4522aeafd3ebc71f9db71eeeef86c4839
4a1c86d5b36c352cc33a0a2c800bc99e62fd65b3a2fd69e0b53996ec13d8ce483ce9319efd9a85acefabdb5342226febb8
3fd1daf4b24265f50c61c6de74077ef89b6fecf9f29a1f871af1e9f89b2d345cda7499bd45c42fa5d195a1e1a6ba8485188
9e730da3b2b916e96152ae0c92154b49719841db7e7cc707ba8a5d7b101eb4ac7b629bb327817910fff61580b59aab78
182d1a2e33473d05b00b170b29e331870826cfe45af206aa7d0246bbd8566ca7cfb2d3c10bfa1db7dd48dd786036469c
e7282093d78b5e1a5b0fc81a54c8ed4ceac1e5305305e78284ac276f5d7862727aff246e17addde50c670028d572cbfc0
be2e4f8b2eb28fa68ad7b4c6c2a239c460441bfb5ea049f23b08563b4e47729a59e5986a61a6093dbd54f8c36ebe87eda
e01f251cb060ad1364ce677d7e8d5a4a4ca966a7241cc360bc2acb280e5f9e9c1b032ad6a180a35e0c5180b9d16d026c8
65b252098cc1d99ba7375ca31c7702c0d943d5e3dd2f6861fa55bd46d94b67ed3e52eccd8dd06d968e01897d6de97ed3
058d91dd":"8e4bc6f8b8c60fe4d68c61d9b159c8693c3151c46749af58da228442d927f23359bd6ccd6c2ec8fa3f00a86
cecbfa728e1ad60b821ed22fcd309ba91a4138bc9"

SHA-1
Selftest
depends_on:MBEDTLS_SELF_TEST:MBEDTLS_SHA1_C
sha1_selftest:

SHA-256 Selftest
depends_on:MBEDTLS_SELF_TEST:MBEDTLS_SHA256_C
sha256_selftest:

SHA-512 Selftest
depends_on:MBEDTLS_SELF_TEST:MBEDTLS_SHA512_C
sha512_selftest:
w<#Na.
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
<ItemGroup Label="ProjectConfigurations">
<ProjectConfiguration Include="Debug|Win32">
<Configuration>Debug</Configuration>
<Platform>Win32</Platform>
</ProjectConfiguration>
<ProjectConfiguration Include="Debug|x64">
<Configuration>Debug</Configuration>
<Platform>x64</Platform>
</ProjectConfiguration>
<ProjectConfiguration Include="Release|Win32">
<Configuration>Release</Configuration>
<Platform>Win32</Platform>
</ProjectConfiguration>

```
  <ProjectConfiguration Include="Release|x64">
    <Configuration>Release</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\test\ssl_cert_test.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">
     <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid>{3FE0C0E1-D9BA-6A26-380C-F293E543B914}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>ssl_cert_test</RootNamespace>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')"
```

```
 Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
    <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
   <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <LinkIncremental>false</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
   <LinkIncremental>false</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <ClCompile>
     <PrecompiledHeader>
     </PrecompiledHeader>
     <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>

  <PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
     <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
     <SubSystem>Console</SubSystem>
     <GenerateDebugInformation>true</GenerateDebugInformation>
     <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
```

```
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
```

```
  </Link>
 </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
  <Import Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
Public key write check RSA
depends_on:MBEDTLS_RSA_C:MBEDTLS_BASE64_C
pk_write_pubkey_check:"data_files/server1.pubkey"

Public key write check RSA 4096
depends_on:MBEDTLS_RSA_C:MBEDTLS_BASE64_C
pk_write_pubkey_check:"data_files/rsa4096_pub.pem"

Public key write check EC 192 bits
depends_on:MBEDTLS_ECP_C:MBEDTLS_BASE64_C:MBEDTLS_ECP_DP_SECP192R1_ENABLED
pk_write_pubkey_check:"data_files/ec_pub.pem"

Public key write check EC 521 bits
depends_on:MBEDTLS_ECP_C:MBEDTLS_BASE64_C:MBEDTLS_ECP_DP_SECP521R1_ENABLED
pk_write_pubkey_check:"data_files/ec_521_pub.pem"

Public key write check EC Brainpool 512 bits
depends_on:MBEDTLS_ECP_C:MBEDTLS_BASE64_C:MBEDTLS_ECP_DP_BP512R1_ENABLED
pk_write_pubkey_check:"data_files/ec_bp512_pub.pem"

Private key write check RSA
depends_on:MBEDTLS_RSA_C:MBEDTLS_BASE64_C
```

pk_write_key_check:"data_files/server1.key"

Private key write check RSA 4096
depends_on:MBEDTLS_RSA_C:MBEDTLS_BASE64_C
pk_write_key_check:"data_files/rsa4096_prv.pem"

Private key write check EC
192 bits
depends_on:MBEDTLS_ECP_C:MBEDTLS_BASE64_C:MBEDTLS_ECP_DP_SECP192R1_ENABLED
pk_write_key_check:"data_files/ec_prv.sec1.pem"

Private key write check EC 521 bits
depends_on:MBEDTLS_ECP_C:MBEDTLS_BASE64_C:MBEDTLS_ECP_DP_SECP521R1_ENABLED
pk_write_key_check:"data_files/ec_521_prv.pem"

Private key write check EC Brainpool 512 bits
depends_on:MBEDTLS_ECP_C:MBEDTLS_BASE64_C:MBEDTLS_ECP_DP_BP512R1_ENABLED
pk_write_key_check:"data_files/ec_bp512_prv.pem"
-----BEGIN CERTIFICATE-----
MIICIDCCAaWgAwIBAgIBCjAKBggqhkjOPQQDAjA+MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EwHhcN
MTMwOTI0MTU1MjA0WhcNMjMwOTIyMTU1MjA0WjA0MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxEjAQBgNVBAMTCWxvY2FsaG9zdDBZMBMGByqGSM49AgEG
CCqGSM49AwEHA0IABIFZMXZJJPoVraugMW4O7TMR+pElVcGwwZwDcj6Yui2kcjeJ
H0M3jR+OOtjwV+gvT8kApPfbcw+yxgSU0UA7OOOjgZ0wgZowCQYDVR0TBAIwADAd
BgNVHQ4EFgQUfmWPPjMDFOXhvmCy4IV/jOdgK3swbgYDVR0jBGcwZYAUnW0gJEkB
PyvLeLUZvH4kydv7NnyhQqRAMD4xCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQb2xh
clNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBFQyBDQYIJAMFD4n5iQ8zoMAoG
CCqGSM49BAMCA2kAMGYCMQCsYTyleBFuI4nizuxo/ie5dxJnD0ynwCnRJ+84PZP4
AQA3HdUz0qNYs4CZ2am9Gz0CMQDr2TNLFA3C3S3pmgXMT0eKzR1Ca1/Nulf0llQZ
Xj09kLboxuemP40IIqhQnpYptMg=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIC6TCCAdGgAwIBAgIBDzANBgkqhkiG9w0BAQsFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTMwOTI0MTYwODQyWhcNMjMwOTIyMTYwODQyWjBLMQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxKTAnBgNVBAMTIFBvbGFyU1NMIFRlc3QgSW50ZXJtZWRp
YXRlIEVDIENBMHYwEAYHKoZIzj0CAQYFK4EEACIDYgAE8Oih3fX5SLeN1dmFncQl
WMw9+Y6sXblhlrXBxhXxjwdwpCHENn+foUVdrqYVYa7Suv3QVeO6nJ19H3QNixW8
ik1P+hxsbaq8bta78vAyHmC4EmXQLg1w7oxb9Q82qX1Yo4GVMIGSMB0GA1UdDgQW
BBQPib1jQevLXhco/2gwPcGI0JxYOTBjBgNVHSMEXDBagBS0WuSls97SUva51aaV
D+s+vMf9/6E/pD0wOzELMAkGA1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NMMRkw
FwYDVQQDExBQb2xhclNTTCBUZXN0IENBggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZI
hvcNAQELBQADggEBAAjeaTUaCBiXT1CYLVr6UFSeRNZBrDPnj6PwqUQTvgB5I5n6
yXqoE4RYDaEL0Lg24juFxI26itBuypto6vscgGq77cfrP/avSdxU+xeZ4bCWvh3M
ddj9lmko2U8I8GhBcHpSuIiTvgKDB8eKkjeq3AsLGchHDvip8pB3IhcNfL7W94Zf
7/lH9VQiE3/px7amD32cidoPvWLA9U3f1FsPmJESUz0wwNfINpDjmPr8dGbkCN+M
CFhxo6sCfK8KLYG4nYX8FwxVR86kpSrO9e84AX0YYbdzxprbc2XOaebJ8+BDmzut

ARkD7DTXrodN1wV7jQJkrUuEwPj9Rhvk+MFRkaw=
-----END
CERTIFICATE-----
-----BEGIN EC PARAMETERS-----
BggqhkjOPQMBBw==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIC8M2G7XcqeagYgt8SZJbuTh4tYchGvX3yDZJKTuBgFUoAoGCCqGSM49
AwEHoUQDQgAEaUHkP2BkI55e0s6OlkrSdbu8bp0y+YwZFx/GgFUptKol+AA/+2D8
WuRJxs2XS059ub0FZ30ABqTMfD9ZWIhmAg==
-----END EC PRIVATE KEY-----
AES-128-ECB Encrypt NIST KAT #1
aes_encrypt_ecb:"00000000000000000000000000000000":"f34481ec3cc627bacd5dc3fb08f273e6":"0336763e966d92595a567cc9ce537f5e":0

AES-128-ECB Encrypt NIST KAT #2
aes_encrypt_ecb:"00000000000000000000000000000000":"9798c4640bad75c7c3227db910174e72":"a9a1631bf4996954ebc093957b234589":0

AES-128-ECB Encrypt NIST KAT #3
aes_encrypt_ecb:"00000000000000000000000000000000":"96ab5c2ff612d9dfaae8c31f30c42168":"ff4f8391a6a40ca5b25d23bedd44a597":0

AES-128-ECB Encrypt NIST KAT #4
aes_encrypt_ecb:"e0000000000000000000000000000000":"00000000000000000000000000000000":"72a1da770f5d7ac4c9ef94d822affd97":0

AES-128-ECB Encrypt NIST KAT #5
aes_encrypt_ecb:"f0000000000000000000000000000000":"00000000000000000000000000000000":"970014d634e2b7650777e8e84d03ccd8":0

AES-128-ECB Encrypt NIST KAT #6
aes_encrypt_ecb:"f8000000000000000000000000000000":"00000000000000000000000000000000":"f17e79aed0db7e279e955b5f493875a7":0

AES-128-ECB Encrypt NIST KAT #7
aes_encrypt_ecb:"fffffffffffff000000000000000000":"00000000000000000000000000000000":"7b90785125505fad59b13c186dd66ce3":0

AES-128-ECB
Encrypt NIST KAT #8
aes_encrypt_ecb:"fffffffffffff800000000000000000":"00000000000000000000000000000000":"8b527a6aebdaec9eaef8eda2cb7783e5":0

AES-128-ECB Encrypt NIST KAT #9
aes_encrypt_ecb:"fffffffffffffc000000000000000000":"00000000000000000000000000000000":"43fdaf53ebbc9880c228617d6a9b548b":0

AES-128-ECB Encrypt NIST KAT #10
aes_encrypt_ecb:"fffffffffffffffffffffffffffffc000":"00000000000000000000000000000000":"70c46bb30692be657f7eaa93ebad9897":0

AES-128-ECB Encrypt NIST KAT #11
aes_encrypt_ecb:"fffffffffffffffffffffffffffffe000":"00000000000000000000000000000000":"323994cfb9da285a5d9642e1759b224a":0

AES-128-ECB Encrypt NIST KAT #12
aes_encrypt_ecb:"ffffffffffffffffffffffffffffff000":"00000000000000000000000000000000":"1dbf57877b7b17385c85d0b54851e371":0

AES-128-ECB Encrypt NIST KAT #13
aes_encrypt_ecb:"00000000000000000000000000000000":"ffffffffffffffc00000000000000000":"3a4d354f02bb5a5e47d39666867f246a":0

AES-128-ECB
Encrypt NIST KAT #14
aes_encrypt_ecb:"00000000000000000000000000000000":"ffffffffffffffe00000000000000000":"d451b8d6e1e1a0ebb155fbbf6e7b7dc3":0

AES-128-ECB Encrypt NIST KAT #15
aes_encrypt_ecb:"00000000000000000000000000000000":"fffffffffffffff00000000000000000":"6898d4f42fa7ba6a10ac05e87b9f2080":0

AES-128-ECB Encrypt NIST KAT #16
aes_encrypt_ecb:"00000000000000000000000000000000":"fffffffffffffffffffffffe0000000":"082eb8be35f442fb52668e16a591d1d6":0

AES-128-ECB Encrypt NIST KAT #17
aes_encrypt_ecb:"00000000000000000000000000000000":"fffffffffffffffffffffff0000000":"e656f9ecf5fe27ec3e4a73d00c282fb3":0

AES-128-ECB Encrypt NIST KAT #18
aes_encrypt_ecb:"00000000000000000000000000000000":"fffffffffffffffffffffff8000000":"2ca8209d63274cd9a29bb74bcd77683a":0

AES-128-ECB Decrypt NIST KAT #1
aes_decrypt_ecb:"00000000000000000000000000000000":"db4f1aa530967d6732ce4715eb0ee24b":"ff00000000000000000000000000000000":0

AES-128-ECB Decrypt NIST KAT
#2
aes_decrypt_ecb:"00000000000000000000000000000000":"a81738252621dd180a34f3455b4baa2f":"ff80000000000000000000000000000000":0

AES-128-ECB Decrypt NIST KAT #3
aes_decrypt_ecb:"00000000000000000000000000000000":"77e2b508db7fd89234caf7939ee5621a":"ffc000000000

00000000000000000000":0

AES-128-ECB Decrypt NIST KAT #4
aes_decrypt_ecb:"00000000000000000000000000000000":"dc43be40be0e53712f7e2bf5ca707209":"6a118a874519e64e9963798a503f1d35":0

AES-128-ECB Decrypt NIST KAT #5
aes_decrypt_ecb:"00000000000000000000000000000000":"92beedab1895a94faa69b632e5cc47ce":"cb9fceec81286ca3e989bd979b0cb284":0

AES-128-ECB Decrypt NIST KAT #6
aes_decrypt_ecb:"00000000000000000000000000000000":"459264f4798f6a78bacb89c15ed3d601":"b26aeb1874e47ca8358ff22378f09144":0

AES-128-ECB Decrypt NIST KAT #7
aes_decrypt_ecb:"b69418a85332240dc82492353956ae0c":"a303d940ded8f0baff6f75414cac5243":"00000000000000000000000000000000":0

AES-128-ECB Decrypt NIST KAT #8
aes_decrypt_ecb:"71b5c08a1993e1362e4d0ce9b22b78d5":"c2dabd117f8a3ecabfbb11d12194d9d0":"00000000000000000000000000000000":0

AES-128-ECB
Decrypt NIST KAT #9
aes_decrypt_ecb:"e234cdca2606b81f29408d5f6da21206":"fff60a4740086b3b9c56195b98d91a7b":"00000000000000000000000000000000":0

AES-128-ECB Decrypt NIST KAT #10
aes_decrypt_ecb:"ffffffffffffffff0000000000000000":"84be19e053635f09f2665e7bae85b42d":"00000000000000000000000000000000":0

AES-128-ECB Decrypt NIST KAT #11
aes_decrypt_ecb:"ffffffffffffffff8000000000000000":"32cd652842926aea4aa6137bb2be2b5e":"00000000000000000000000000000000":0

AES-192-ECB Encrypt NIST KAT #1
aes_encrypt_ecb:"000000000000000000000000000000000000000000000000":"ffffffffffffffffffff80000000000":"156f07767a85a4312321f63968338a01":0

AES-192-ECB Encrypt NIST KAT #2
aes_encrypt_ecb:"000000000000000000000000000000000000000000000000":"ffffffffffffffffffffc0000000000":"15eec9ebf42b9ca76897d2cd6c5a12e2":0

AES-192-ECB Encrypt NIST KAT #3
aes_encrypt_ecb:"000000000000000000000000000000000000000000000000":"ffffffffffffffffffffe0000000000":"db0d3a6fdcc13f915e2b302ceeb70fd8":0

AES-192-ECB

Encrypt NIST KAT #4
aes_encrypt_ecb:"000000000000000000000000000000000000000000000000":"51719783d3185a535bd75adc65071ce1":"4f354592ff7c8847d2d0870ca9481b7c":0

AES-192-ECB Encrypt NIST KAT #5
aes_encrypt_ecb:"000000000000000000000000000000000000000000000000":"26aa49dcfe7629a8901a69a9914e6dfd":"d5e08bf9a182e857cf40b3a36ee248cc":0

AES-192-ECB Encrypt NIST KAT #6
aes_encrypt_ecb:"000000000000000000000000000000000000000000000000":"941a4773058224e1ef66d10e0a6ee782":"067cd9d3749207791841562507fa9626":0

AES-192-ECB Encrypt NIST KAT #7
aes_encrypt_ecb:"d2926527e0aa9f37b45e2ec2ade5853ef807576104c7ace3":"00000000000000000000000000000000":"dd619e1cf204446112e0af2b9afa8f8c":0

AES-192-ECB Encrypt NIST KAT #8
aes_encrypt_ecb:"982215f4e173dfa0fcffe5d3da41c4812c7bcc8ed3540f93":"00000000000000000000000000000000":"d4f0aae13c8fe9339fbf9e69ed0ad74d":0

AES-192-ECB Encrypt NIST KAT #9
aes_encrypt_ecb:"98c6b8e01e379fbd14e61af6af891596583565f2a27d59e9":"00000000000000000000000000000000":"19c80ec4a6deb7e5ed1033dda933498f":0

AES-192-ECB
Encrypt NIST KAT #10
aes_encrypt_ecb:"ffffffffffffffffffffffffffff80000000000000000000":"00000000000000000000000000000000":"8dd274bd0f1b58ae345d9e7233f9b8f3":0

AES-192-ECB Encrypt NIST KAT #11
aes_encrypt_ecb:"ffffffffffffffffffffffffffffc0000000000000000000":"00000000000000000000000000000000":"9d6bdc8f4ce5feb0f3bed2e4b9a9bb0b":0

AES-192-ECB Encrypt NIST KAT #12
aes_encrypt_ecb:"ffffffffffffffffffffffffffffe0000000000000000000":"00000000000000000000000000000000":"fd5548bcf3f42565f7efa94562528d46":0

AES-192-ECB Decrypt NIST KAT #1
aes_decrypt_ecb:"ffffffffffffffffffffffffffffffffffffff000000000000000":"bb2852c891c5947d2ed44032c421b85f":"00000000000000000000000000000000":0

AES-192-ECB Decrypt NIST KAT #2
aes_decrypt_ecb:"ffffffffffffffffffffffffffffffffffffff800000000000000":"1b9f5fbd5e8a4264c0a85b80409afa5e":"00000000000000000000000000000000":0

AES-192-ECB Decrypt NIST KAT #3
aes_decrypt_ecb:"ffffffffffffffffffffffffffffffffffffc00000000000000":"30dab809f85a917fe924733f424ac589":"00000000000000000000000000000000":0

AES-192-ECB
Decrypt NIST KAT #4
aes_decrypt_ecb:"61257134a518a0d57d9d244d45f6498cbc32f2bafc522d79":"cfe4d74002696ccf7d87b14a2f9cafc9
":"00000000000000000000000000000000":0

AES-192-ECB Decrypt NIST KAT #5
aes_decrypt_ecb:"b0ab0a6a818baef2d11fa33eac947284fb7d748cfb75e570":"d2eafd86f63b109b91f5dbb3a3fb7e13"
:"00000000000000000000000000000000":0

AES-192-ECB Decrypt NIST KAT #6
aes_decrypt_ecb:"ee053aa011c8b428cdcc3636313c54d6a03cac01c71579d6":"9b9fdd1c5975655f539998b306a324a
f":"00000000000000000000000000000000":0

AES-192-ECB Decrypt NIST KAT #7
aes_decrypt_ecb:"000000000000000000000000000000000000000000000000":"275cfc0413d8ccb70513c3859b1d0
f72":"1b077a6af4b7f98229de786d7516b639":0

AES-192-ECB Decrypt NIST KAT #8
aes_decrypt_ecb:"000000000000000000000000000000000000000000000000":"c9b8135ff1b5adc413dfd053b21bd9
6d":"9c2d8842e5f48f57648205d39a239af1":0

AES-192-ECB Decrypt NIST
KAT #9
aes_decrypt_ecb:"000000000000000000000000000000000000000000000000":"4a3650c3371ce2eb35e389a171427
440":"bff52510095f518ecca60af4205444bb":0

AES-192-ECB Decrypt NIST KAT #10
aes_decrypt_ecb:"000000000000000000000000000000000000000000000000":"b2099795e88cc158fd75ea133d7e7f
be":"ffffffffffffffffffffc00000000000":0

AES-192-ECB Decrypt NIST KAT #11
aes_decrypt_ecb:"000000000000000000000000000000000000000000000000":"a6cae46fb6fadfe7a2c302a3424281
7b":"ffffffffffffffffffffe00000000000":0

AES-192-ECB Decrypt NIST KAT #12
aes_decrypt_ecb:"000000000000000000000000000000000000000000000000":"026a7024d6a902e0b3ffccbaa910cc
3f":"fffffffffffffffffffff00000000000":0

AES-256-ECB Encrypt NIST KAT #1
aes_encrypt_ecb:"c1cc358b449909a19436cfbb3f852ef8bcb5ed12ac7058325f56e6099aab1a1c":"000000000000000
00000000000000000":"352065272169abf9856843927d0674fd":0

AES-256-ECB Encrypt NIST KAT #2
aes_encrypt_ecb:"984ca75f4ee8d706f46c2d98c0bf4a45f5b00d791c2dfeb191b5ed8e420fd627":"000000000000000
00000000000000000":"4307456a9e67813b452e15fa8fffe398":0

AES-256-ECB

Encrypt NIST KAT #3
aes_encrypt_ecb:"b43d08a447ac8609baadae4ff12918b9f68fc1653f1269222f123981ded7a92f":"0000000000000000
0000000000000000":"46634466073549894 77a5c6f0f007ef4":0

AES-256-ECB Encrypt NIST KAT #4
aes_encrypt_ecb:"0000000000000000000000000000000000000000000000000000000000000000":"0b24af36193ce
4665f2825d7b4749c98":"a9ff75bd7cf6613d3731c77c3b6d0c04":0

AES-256-ECB Encrypt NIST KAT #5
aes_encrypt_ecb:"0000000000000000000000000000000000000000000000000000000000000000":"761c1fe41a18a
cf20d241650611d90f1":"623a52fcea5d443e48d9181ab32c7421":0

AES-256-ECB Encrypt NIST KAT #6
aes_encrypt_ecb:"0000000000000000000000000000000000000000000000000000000000000000":"8a560769d605
868ad80d819bdba03771":"38f2c7ae10612415d27ca190d27da8b4":0

AES-256-ECB Encrypt NIST KAT #7
aes_encrypt_ecb:"0000000000000000000000000000000000000000000000000000000000000000":"ffffff8000000
0000000000000000000":"36aff0ef7bf3280772cf4cac80a0d2b2":0

AES-256-ECB Encrypt
NIST KAT #8
aes_encrypt_ecb:"0000000000000000000000000000000000000000000000000000000000000000":"fffffc0000000
0000000000000000000":"1f8eedea0f62a1406d58cfc3ecea72cf":0

AES-256-ECB Encrypt NIST KAT #9
aes_encrypt_ecb:"0000000000000000000000000000000000000000000000000000000000000000":"fffffe0000000
0000000000000000000":"abf4154a3375a1d3e6b1d454438f95a6":0

AES-256-ECB Encrypt NIST KAT #10
aes_encrypt_ecb:"ffffffffffffffffffffffffffffffff80000000000000000000000000000000":"0000000000000000000000000
00000000":"45d089c36d5c5a4efc689e3b0de10dd5":0

AES-256-ECB Encrypt NIST KAT #11
aes_encrypt_ecb:"ffffffffffffffffffffffffffffffffc0000000000000000000000000000000":"0000000000000000000000000
00000000":"b4da5df4becb5462e03a0ed00d295629":0

AES-256-ECB Encrypt NIST KAT #12
aes_encrypt_ecb:"ffffffffffffffffffffffffffffffffe0000000000000000000000000000000":"0000000000000000000000000
00000000":"dcf4e129136c1a4b7a0f38935cc34b2b":0

AES-256-ECB Decrypt NIST KAT #1
aes_decrypt_ecb:"ffffffffffffffffffffffffffffffffffffffffffffffff0000000000000000":"edf61ae362e882ddc0167474a7a77
f3a":"00000000000000000000000000000000":0

AES-256-ECB
Decrypt NIST KAT #2
aes_decrypt_ecb:"ffffffffffffffffffffffffffffffffffffffffffffffff8000000000000000":"6168b00ba7859e0970ecfd757efecf

7c":"00000000000000000000000000000000":0

AES-256-ECB Decrypt NIST KAT #3
aes_decrypt_ecb:"ffffffffffffffffffffffffffffffffffffffffffffffffc0000000000000000":"d1415447866230d28bb1ea18a4cdfd02":"00000000000000000000000000000000":0

AES-256-ECB Decrypt NIST KAT #4
aes_decrypt_ecb:"f8be9ba615c5a952cabbca24f68f8593039624d524c816acda2c9183bd917cb9":"a3944b95ca0b52043584ef02151926a8":"00000000000000000000000000000000":0

AES-256-ECB Decrypt NIST KAT #5
aes_decrypt_ecb:"797f8b3d176dac5b7e34a2d539c4ef367a16f8635f6264737591c5c07bf57a3e":"a74289fe73a4c123ca189ea1e1b49ad5":"00000000000000000000000000000000":0

AES-256-ECB Decrypt NIST KAT #6
aes_decrypt_ecb:"6838d40caf927749c13f0329d331f448e202c73ef52c5f73a37ca635d4c47707":"b91d4ea4488644b56cf0812fa7fcf5fc":"00000000000000000000000000000000":0

AES-256-ECB
Decrypt NIST KAT #7
aes_decrypt_ecb:"0000000000000000000000000000000000000000000000000000000000000000":"623a52fcea5d443e48d9181ab32c7421":"761c1fe41a18acf20d241650611d90f1":0

AES-256-ECB Decrypt NIST KAT #8
aes_decrypt_ecb:"0000000000000000000000000000000000000000000000000000000000000000":"38f2c7ae10612415d27ca190d27da8b4":"8a560769d605868ad80d819bdba03771":0

AES-256-ECB Decrypt NIST KAT #9
aes_decrypt_ecb:"0000000000000000000000000000000000000000000000000000000000000000":"1bc704f1bce135ceb810341b216d7abe":"91fbef2d15a97816060bee1feaa49afe":0

AES-256-ECB Decrypt NIST KAT #10
aes_decrypt_ecb:"0000000000000000000000000000000000000000000000000000000000000000":"ddc6bf790c15760d8d9aeb6f9a75fd4e":"80000000000000000000000000000000":0

AES-256-ECB Decrypt NIST KAT #11
aes_decrypt_ecb:"0000000000000000000000000000000000000000000000000000000000000000":"0a6bdc6d4c1e6280301fd8e97ddbe601":"c0000000000000000000000000000000":0

AES-256-ECB
Decrypt NIST KAT #12
aes_decrypt_ecb:"0000000000000000000000000000000000000000000000000000000000000000":"9b80eefb7ebe2d2b16247aa0efc72f5d":"e0000000000000000000000000000000":0
-----BEGIN X509 CRL-----
MIIBqzCBlDANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDERMA8GA1UEChMI
UG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EXDTExMDIyMDEwMjI1
OVoXDTE5MTEyNTEwMjI1OVowKDASAgEBFw0xMTAyMTIxNDQ0MDdaMBICAQMXDTEx
MDIxMjE0NDQwN1owDQYJKoZIhvcNAQEFBQADggEBAJYuWdKPdblMVWCnxpMnchuL

dqWzK2BA0RelCaGjpxuwX3NmLDm+5hKja/DJxaRqTOf4RSC3kcX8CdIldsLO96dz
//wAQdFPDhy6AFT5vKTO8ItPHDb7qFOqFqpeJi5XN1yoZGTB1ei0mgD3xBaKbp6U
yCOZJSIFomt7piT4GcgWVHLUmpyHDDeodNhYPrN0jf2mr+ECd9fQJYdz1qm0Xx+Q
NbKXDiPRmPX0qVleCZSeSp1JAmU4GoCO+96qQUpjgll+6xWya3UNj61f9sh0Zzr7
5ug2LZo5uBM/LpNR1K3TLxNCcg7uUPTn9r143d7ivJhPl3tEJn4PXjv6mlLoOgU
-----END X509 CRL-----
-----BEGIN X509 CRL-----
MIIBcTCB9wIBATAKBggqhkjOPQQDAjA+MQswCQYDVQQGEwJOTDERMA8GA1UEChMI
UG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EXDTEzMDkyNDE2
MzEwOFoXDTIzMDkyMjE2MzEwOFowFDASAgEKFw0xMzA5MjQxNjI4MzhaoHIwcDBu
BgNVHSMEZzBlgBSdbSAkSQE/K8t4tRm8fiTJ2/s2fKFCpEAwPjELMAkGA1UEBhMC
TkwxETAPBgNVBAoTCFBvbGFyU1NMMRwwGgYDVQQDExNQb2xhcnNzbCBUZXN0IEVD
IENBggkAwUPifmJDzOgwCgYIKoZIzj0EAwIDaQAwZgIxAKuQ684s7gyhtxKJr6Ln
S2BQ02f1jjPHrZVdXaZvm3C5tGi2cKkoK1aMiyC3LsRCuAIxAIMhj0TmcuIZr5fX
g5RByD7zUnZBpoEAdgxFy4JPJ2IViWOPekSGh8b/JY1VNS6Zbw==
-----END
X509 CRL-----
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-256-CBC,53572EEEE794948AC48CB0E077CE075A

p0YobpQmzHb3NgGlojpYoH+G5f1XX9snYv2GQe2tGTBQpoHh+ivHcOt85EZu9pC1
1KRdALEwp7Cb4RYeQncV9Bfp5rItupS1TwfgKAlp7Plmb4vDcDVw+KL3PaYn52Bd
qq5USLxCvKcl91hZXzitttH072lEj2MzW2QpX2/1hCRPgMDu9PJlBX2S+GOaYP+9
sTWTCc1yvHMW4XGEM4P4yfRg9EOTxU5gIYWUE2JqmEGd+9I0hK2YevAPLNKHxzpy
klCCBYqDplcVT5zEyCmdiBHIjzodlFuocZC8ncinVnsuJvpTeMQ+zOZ5rao8xm2j
uCnnVRh7yZktfsf5B/ZKBMGyPYRyKN4CCYhF0GzbehTvBirgDELq4LHyDdnnOTwU
YJiqo17x6S4FVNq6AubADVAbCOMFyfr+TFshI8spOwqfGFFDs8/WWL5OnBS85Pd1
dgoqwzJAt55GyDUbGnp6hUFl9g96nvV3sE6Xe4xVE2Cpf1BtUl9Dt3UrrDrbS0dk
pKxl2FA2H0BVKtfNBHXvWkORi+v+XZl34rZZ37B8snYIN2aOqLuvyM4fd1EabkyG
ymMEUHJcrc5zl/7IECaHrCahqZIsLpLhGTd0MMGrkGSvRLiY5nQ4MN5tKI0fUw0S
5KIjOA6ZX5nvh4rYgQcgN7K6dXNA2hOj5256Vv0HVwXsVhQFmCGnuo+h8XxudRVH
RuIUaTUtl29a/2nPTzXB6MNZe7Wol8EkzuYEgyaizKr7nO0J1umg+lj7ipX/80Ji
3ADi0yL4F831LsdAiTY60Lu2e3WABleZsvuLMWSodb9WzJXknsnFEDLGOM+HGj8Q
-----END RSA PRIVATE KEY-----
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQDMYfnvWtC8Id5bPKae5yXSxQTt+Zpul6AnnZWfI2TtIarvjHBF
UtXRo96y7hoL4VWOPKGCsRqMFDkrbeUjRrx8iL914/srnyf6sh9c8Zk04xEOpK1y
pvBz+Ks4uZObtjnnitf0NBGdjMKxveTq+VE7BWUIyQjtQ8mbDOsiLLvh7wIDAQAB
AoGAefPIT8MPpAJNjIE/JrfkAMTgsSLrvCurO5gzDBbxhPE+7tsMrsDDpuix3HBo
iEg3ZbzV3obQwV7b0gcr34W4t0CMuJf5b5irHRG8JcZuncmofDy6z7S5Vs75O85z
fVzTIuVUyuHy1rM6rSBYKfsMLVyImUb4wtIXEMHPzdCL9LECQQD3ZfgGqudMWq8v
3BlKhsQ4fsR0vxzNlMZfoRrZzcvBT339Bp1UQ8aUo8xBtHiRwuW1NaPNgYKX6XQ6
ppuWuTiJAkEA030i493KnFPLRwWypqF/s6ZNlVye+euFN5NF/IeJcvb/GUDRYv9O
pRozRS1jNx4ZB1K2xT7N9MwsPHD6j6K4twJBALdfHTfT9RzjGnae7SAQQ+CcFYFz
JiY6386B2yUVJLFj+j5RaMvMcKQ7xGnvGm7vxtNJrt/j3qg6oavXUfulzgECQQDP
CEVLhCd/+ZeZoz5MWPTGTRrOCKmoRqNW0FlG6PfpD1qSwh04KG44uflO0yu5HUGr
JZG+bcj4x5bWZFMkoUrpAkEAyEgQzesKFqcbt1cqv3pLXJYQBBw6leFXgHk11a7k

+AkexhrPYyq/4tXFO2TLk2hs7tpYgNDOqZCvEu7jtN3RuA==
-----END RSA PRIVATE KEY-----
-----BEGIN EC PARAMETERS-----
BggqhkjOPQMBBw==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEINSnxPqUNMba8F2KWNxU88heSs7vgas5BOzjRwQsQe6IoAoGCCqGSM49
AwEHoUQDQgAEM55/cxx8CxjvFUeFvVe7zJcQnaKI8xDol+WOibT7RTs/Ournh2Os
6DdP5ieg56p0l4pSSFFHlunhn6ppGu58ZA==
-----END EC PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIBtDCCATqgAwIBAgIBTTAKBggqhkjOPQQDAjBLMQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxKTAnBgNVBAMTIFBvbGFyU1NMIFRlc3QgSW50ZXJtZWRp
YXRlIEVDIENBMB4XDTE1MDkwMTE0MDg0M1oXDTI1MDgyOTE0MDg0M1owSjELMAkG
A1UEBhMCVUsxETAPBgNVBAoTCG1iZWQgVExTMSgwJgYDVQQDEx9tYmVkIFRMUyBU
ZXN0IGludGVybWVkaWF0ZSBDQSAzMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE
732fWHLNPMPsP1U1ibXvb55erlEVMlpXBGsj+KYwVqU1XCmW9Z9hhP7X/5js/DX9
2J/utoHyjUtVpQOzdTrbsaMQMA4wDAYDVR0TBAUwAwEB/zAKBggqhkjOPQQDAgNo
ADBlAjAJRxbGRas3NBmk9MnGWXg7PT1xnRELHRWWIvfLdVQt06l1/xFg3ZuPdQdt
Qh7CK80CMQD7wa1o1a8qyDKBfLN636uKmKGga0E+vYXBeFCy9oARBangGCB0B2vt
pz590JvGWfM=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDwjCCAaqgAwIBAgIBEDANBgkqhkiG9w0BAQsFADBIMQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxJjAkBgNVBAMTHVBvbGFyU1NMIFRlc3QgSW50ZXJt
ZWRpYXRlIENBMB4XDTEzMDkyNDE2MTIyNFoXDTIzMDkyMjE2MTIyNFowNDELMAkG
A1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NMMRIwEAYDVQQDEwlsb2NhbGhvc3Qw
WTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQcbffp2qXqoZyychmoCRxzrd4Vu96m
47NPBehtEC46aTeXgDnBdf++znABrAtfXBRNQz8ARIeYBmskr22rlKjyo4GVMIGS
MAkGA1UdEwQCMAAwHQYDVR0OBBYEFNIK06V3H85VsFxGoo5zbL+hYCa7MGYGA1Ud
IwRfMF2AFDh32Gt3nCh3gotO2BupHveUFrcOoUKkQDA+MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0GC
AQ4wDQYJKoZIhvcNAQELBQADggIBADRoQ5fHKw+vkl0D3aqLX1XrZidb+25AWbhr
FYXdaskN219PrXBL3cV8x5tK6qsPKSyyw1lue80OmhXs/w7PJkOHHUSWRnmTv7lr
8Us3Zr/yOF/VVqzdGs7DlOTpyzEBdugI9uar/aCqHDoltN8wOduOoQB9aojYpROj
+gjlEO0mgt/87XpjYOig1o0jv44QYDQZQzpj1zeIn6WMe6xk9YDwCLMjRIpg++c7
QyxvcEJTn80wX1SaEBM2gau97G7bORLMwBVkMT4oSY+iKYgpPpawOnMJbqUP73Dm
yfJExDdrW/BbWZ/vKIcSqSZIbkHdkNjUDVHczyVwQxZxzvLFw/B1k9s7jYFsi5eK
TNAdXFa4et1H2sd+uhu24GxsjmJioDrftixcgzPVBjDCjH8QWkBEX292WJ58on0e
deWLpZUnzPdE1B4rsiPw1Vg28mGgr2O1xgBQr/fx6A+8ItNTzAXbZfEcult9ypwM
0b6YDNe5IvdKk8iwz3mof0VNy47K6xoCaE/fxxWkjoXK8x2wfswGeP2QgUzQE93b
OtjdHpsG1c7gIVFQmKATyAPUz4vqmezgNRleXU0oL0PYtoCmKQ51UjNMUfmO9xCj
VJaNa2iTQ5Dgic+CW4TYAgj5/9g9X3WfwnDNxrZ0UxxawGElczHXqbrNleTtPaKp
a8Si6UK5
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEATCCA4egAwIBAgIBDjAKBggqhkjOPQQDAjA+MQswCQYDVQQGEwJOTDERMA8G

A1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EwHhcN
MTMwOTI0MTU1NTE0WhcNMjMwOTIyMTU1NTE0WjBIMQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxJjAkBgNVBAMTHVBvbGFyU1NMIFRlc3QgSW50ZXJtZWRp
YXRlIENBMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAo1Oc8nr6fMTq
vowV+CpC55i5BZGFGc50Eb4RLBSRTH1e7JepdFjAVbBtyQRJSiY1ja0tgLQDDKZR
wfEI+b4azse460InPHv7C1TN0upXlxuj6m9B1IlP+sBaM7WBC6dVfPO+jVMIxgkF
CaBCLhhdK1Fjf8HjkT/PkctWnho8NTwivc9+nqRZjXe/eIcqm5HwjDDhu+gz+o0g
Vz9MfZNi1JyCrOyNZcy+cr2QeNnNVGnFq8xTxtu6dLunhpmLFj2mm0Vjwa7Ypj5q
AjpqTMtDvqbRuToyoyzajhMNcCAf7gwzIupJJFVdjdtgYAcQwzikwF5HoITJzzJ2
qgxF7CmvGZNb7G99mLdLdhtclH3wAQKHYwEGJo7XKyNEuHPQgB+e0cg1SD1HqlAM
uCfGGTWQ6me7Bjan3t0NzoTdDq6IpKTesbaY+/9e2xn8DCrhBKLXQMZFDZqUoLYA
kGPOEGgvlPnIIXAawouxCaNYEh5Uw871YMSPT28rLdFr49dwYOtDg9foA8hDIW2P
d6KXbrZteesvA1nYzEOs+3AjrbT79Md2W8Bz9bqBVNlNOESSqm4kiCJFmslm/6br
Np0MSQd+o22PQ4xRtmP6UsTfU0ueiMpYc8TYYhMbfnfFyo4m707ebcflPbBEN2dg
updQ66cvfCJB0QJt9upafY0lpdV1qUkCAwEAAaOBoDCBnTAdBgNVHQ4EFgQUOHfY
a3ecKHeCi07YG6ke95QWtw4wbgYDVR0jBGcwZYAUnW0gJEkBPyvLeLUZvH4kydv7
NnyhQqRAMD4xCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEcMBoGA1UE
AxMTUG9sYXJzc2wgVGVzdCBFQyBDQYIJAMFD4n5iQ8zoMAwGA1UdEwQFMAMBAf8w
CgYIKoZIzj0EAwIDaAAwZQIxAPyE+u+eP7gRrSFjQicmpYg8jiFUCYEowWY2zuOG
i1HXYwmpDHfasQ3rNSuf/gHvjwIwbSSjumDk+uYNci/KMELDsD0MFHxZhhBc9Hp9
Af5cNR8KhzegznL6amRObGGKmX1F
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE REQUEST-----
MIICgTCCAWkCAQAwPDELMAkGA1UEBhMCTkwxETAPBgNVBAoTCFBvbGFyU1NMMRow
GAYDVQQDExFQb2xhclNTTCBTZXJ2ZXIgMTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAKkCHz1AatVVU4v9Nu6CZS4VYV6Jv7joRZDb7ogWUtPxQ1BHlhJZ
ZIdr/SvgRvlzvt3PkuGRW+1moG+JKXlFgNCDatVBQ3dfOXwJBEeCsFc5cO2j7BUZ
HqgzCEfBBUKp/UzDtN/dBh9NEFFAZ3MTD0D4bYElXwqxU8YwfhU5rPla7n+SnqYF
W+cTl4W1I5LZ1CQG1QkliXUH3aYajz8JGb6tZSxk65Wb3P5BXhem2mxbacwCuhQs
FiScStzN0PdSZ3PxLaAj/X70McotcMqJCwTbLqZPcG6ezr1YieJTWZ5uWpJl4og/
DJQZo93l6J2VE+0p26twEtxaymsXq1KCVLECAwEAAaAAMA0GCSqGSIb3DQEBAwUA
A4IBAQAPPUzYvUA+HQTteMhkGcuD6XtsZ3i2gQdDGgLUxtMAVFw+/5ZS6l+WqPgq
WQIOsEINPHnjUAMz5pjbFdFqu7X5G29THa2da0Ua2bJO/bu3CZ6EksGmclqaQ2Zl
vfkWaI3bfPFh8eKHF+F5oaVp0gHviCakNqxot4rrZdL8pnJC5JJ+f76y6SgHYOao
SGCv1gYURhIsX0gWCqldsCwxJQFEig9HISUcXViGGVnLdshUtuKL9yNZ/HNAOuOk
7N7a7ur8KMmvar1jkTq+zKSSuSrzmU2JvxFdqU0Gr7A35jgnVG8sj66L4lAcwdoG
sP8OmC1hWh4U3avH6EHdEG8lw0U7
-----END CERTIFICATE REQUEST-----
-----BEGIN X509 CRL-----
MIIBbzCB9gIBATAJBgcqhkjOPQQBMD4xCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQ
b2xhclNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBFQyBDQRcNMTMwOTI0MTYz
MTA4WhcNMjMwOTIyMTYzMTA4WjAUMBICAQoXDTEzMDkyNDE2MjgzOFqgcjBwMG4G
A1UdIwRnMGWAFJ1tICRJAT8ry3i1Gbx+JMnb+zZ8oUKkQDA+MQswCQYDVQQGEwJO
TDERMA8GA1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMg
Q0GCCQDBQ+J+YkPM6DAJBgcqhkjOPQQBA2kAMGYCMQDVG95rrSSl4dJgbJ5vR1GW
svEuEsAh35EhF1WrcadMuCeMQVX9cUPupFfQUpHyMfoCMQCKf0yv8pN9BAoi3FVm
56meWPhUekgLKKMAobt2oJJY6feuiFU2YFGs1aF0rV6Bj+U=

-----END X509 CRL-----
PBKDF2 RFC 6070 Test Vector #1 (SHA1)
depends_on:MBEDTLS_SHA1_C
pbkdf2_hmac:MBEDTLS_MD_SHA1:"70617373776f7264":"73616c74":1:20:"0c60c80f961f0e71f3a9b524af6012062fe037a6"

PBKDF2 RFC 6070 Test Vector #2 (SHA1)
depends_on:MBEDTLS_SHA1_C
pbkdf2_hmac:MBEDTLS_MD_SHA1:"70617373776f7264":"73616c74":2:20:"ea6c014dc72d6f8ccd1ed92ace1d41f0d8de8957"

PBKDF2 RFC 6070 Test Vector #3 (SHA1)
depends_on:MBEDTLS_SHA1_C
pbkdf2_hmac:MBEDTLS_MD_SHA1:"70617373776f7264":"73616c74":4096:20:"4b007901b765489abead49d926f721d065a429c1"

PBKDF2 RFC 6070 Test Vector #5 (SHA1)
depends_on:MBEDTLS_SHA1_C
pbkdf2_hmac:MBEDTLS_MD_SHA1:"70617373776f726450415353574f524470617373776f7264":"73616c7453414c5473616c7453414c5473616c7453414c5473616c7453414c5473616c74":4096:25:"3d2eec4fe41c849b80c8d83662c0e44a8b291a964cf2f07038"

PBKDF2 RFC 6070 Test Vector #6 (SHA1)
depends_on:MBEDTLS_SHA1_C
pbkdf2_hmac:MBEDTLS_MD_SHA1:"7061737300776f7264":"7361006c74":4096:16:"56fa6aa75548099dcc37d7f03425e0c3"

PBES2 Decrypt (OK)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC
mbedtls_pkcs5_pbes2:MBEDTLS_ASN1_CONSTRUCTED
|
MBEDTLS_ASN1_SEQUENCE:"301B06092A864886F70D01050C300E04082ED7F24A1D516DD702020800301406082A864886F70D030704088A4FCC9DCC394910":"70617373776f7264":"1B60098D4834CA752D37B430E70B7A085CFF86E21F4849F969DD1DF623342662443F8BD1252BF83CEF6917551B08EF55A69C8F2BFFC93BCB2DFE2E354DA28F896D1BD1BFB972A1251219A6EC7183B0A4CF2C4998449ED786CAE2138437289EB2203974000C38619DA57A4E685D29649284602BD1806131772DA11A682674DC22B2CF109128DDB7FD980E1C5741FC0DB7":0:"3081870201003013060728A8648CE3D020106082A8648CE3D030107046D306B0201010420F12A1320760270A83CBFFD53F6031EF76A5D86C8A204F2C30CA9EBF51F0F0EA7A1440342000437CC56D976091E5A723EC7592DFF206EEE7CF9069174D0AD14B5F768225962924EE500D82311FFEA2FD2345D5D16BD8A88C26B770D55CD8A2A0EFA01C8B4EDFF060606060606"

PBES2 Decrypt (bad params tag)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_DES_C
mbedtls_pkcs5_pbes2:MBEDTLS_ASN1_SEQUENCE:"":"":"":MBEDTLS_ERR_PKCS5_INVALID_FORMAT + MBEDTLS_ERR_ASN1_UNEXPECTED_TAG:""

PBES2

Decrypt (bad KDF AlgId: not a sequence)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_DES_C
mbedtls_pkcs5_pbes2:MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:"31":"":"":MBEDTLS_ERR_PKCS5_INVALID_FORMAT +
MBEDTLS_ERR_ASN1_UNEXPECTED_TAG:""

PBES2 Decrypt (bad KDF AlgId: overlong)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_DES_C
mbedtls_pkcs5_pbes2:MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:"3001":"":"":MBEDTLS_ERR_PKCS5_INVALID_FORMAT +
MBEDTLS_ERR_ASN1_OUT_OF_DATA:""

PBES2 Decrypt (KDF != PBKDF2)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_DES_C
mbedtls_pkcs5_pbes2:MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:"300B06092A864886F70D01050D":"":"":MBEDTLS_ERR_PKCS5_FEATURE
_UNAVAILABLE:""

PBES2 Decrypt (bad PBKDF2 params: not a sequence)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_DES_C
mbedtls_pkcs5_pbes2:MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:"300D06092A864886F70D01050C3100":"":"":MBEDTLS_ERR_PKCS5_INVA
LID_FORMAT + MBEDTLS_ERR_ASN1_UNEXPECTED_TAG:""

PBES2 Decrypt (bad PBKDF2 params:
overlong)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_DES_C
mbedtls_pkcs5_pbes2:MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:"300D06092A864886F70D01050C3001":"":"":MBEDTLS_ERR_PKCS5_INVA
LID_FORMAT + MBEDTLS_ERR_ASN1_OUT_OF_DATA:""

PBES2 Decrypt (bad PBKDF2 params salt: not an octet string)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC
mbedtls_pkcs5_pbes2:MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:"300E06092A864886F70D01050C30010500":"":"":MBEDTLS_ERR_PKCS5_I
NVALID_FORMAT + MBEDTLS_ERR_ASN1_UNEXPECTED_TAG:""

PBES2 Decrypt (bad PBKDF2 params salt: overlong)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_DES_C
mbedtls_pkcs5_pbes2:MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:"300E06092A864886F70D01050C30010401":"":"":MBEDTLS_ERR_PKCS5_I
NVALID_FORMAT + MBEDTLS_ERR_ASN1_OUT_OF_DATA:""

PBES2 Decrypt (bad PBKDF2 params iter: not an int)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_DES_C
mbedtls_pkcs5_pbes2:MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:"301906092A864886F70D01050C300C04082ED7F24A1D516DD70300":"":"
MBEDTLS_ERR_PKCS5_INVALID_FORMAT

+ MBEDTLS_ERR_ASN1_UNEXPECTED_TAG:""

PBES2 Decrypt (bad PBKDF2 params iter: overlong)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_DES_C
mbedtls_pkcs5_pbes2:MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:"301906092A864886F70D01050C300C04082ED7F24A1D516DD70201":"":"":
MBEDTLS_ERR_PKCS5_INVALID_FORMAT + MBEDTLS_ERR_ASN1_OUT_OF_DATA:""

PBES2 Decrypt (OK, PBKDF2 params explicit keylen)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC
mbedtls_pkcs5_pbes2:MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:"301E06092A864886F70D01050C301104082ED7F24A1D516DD702020800020
118301406082A864886F70D030704088A4FCC9DCC394910":"70617373776f7264":"1B60098D4834CA752D37
B430E70B7A085CFF86E21F4849F969DD1DF623342662443F8BD1252BF83CEF6917551B08EF55A69C8F2BF
FC93BCB2DFE2E354DA28F896D1BD1BFB972A1251219A6EC7183B0A4CF2C4998449ED786CAE213843728
9EB2203974000C38619DA57A4E685D29649284602BD1806131772DA11A682674DC22B2CF109128DDB7FD9
80E1C5741FC0DB7":0:"308187020100301306072A8648CE3D020106082A8648CE3D030107046D306B0201010
420F12A1320760270A83CBFFD53F6031EF76A5D86C8A204F2C30CA9EBF51F0F0EA7A1440342000437CC56
D976091E5A723EC7592DFF206EEE7CF9069174D0AD14B5F768225962924EE500D82311FFEA2FD2345D5D1
6BD8A88C26B770D55CD8A2A0EFA01C8B4EDFF060606060606"

PBES2
Decrypt (bad PBKDF2 params explicit keylen: overlong)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_DES_C
mbedtls_pkcs5_pbes2:MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:"301D06092A864886F70D01050C301004082ED7F24A1D516DD702020800020
1":"":"":MBEDTLS_ERR_PKCS5_INVALID_FORMAT + MBEDTLS_ERR_ASN1_OUT_OF_DATA:""

PBES2 Decrypt (OK, PBKDF2 params explicit prf_alg)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC
mbedtls_pkcs5_pbes2:MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:"302706092A864886F70D01050C301A04082ED7F24A1D516DD702020800300
A06082A864886F70D0207301406082A864886F70D030704088A4FCC9DCC394910":"70617373776f7264":"1B6
0098D4834CA752D37B430E70B7A085CFF86E21F4849F969DD1DF623342662443F8BD1252BF83CEF6917551
B08EF55A69C8F2BFFC93BCB2DFE2E354DA28F896D1BD1BFB972A1251219A6EC7183B0A4CF2C4998449
ED786CAE2138437289EB2203974000C38619DA57A4E685D29649284602BD1806131772DA11A682674DC22
B2CF109128DDB7FD980E1C5741FC0DB7":0:"308187020100301306072A8648CE3D020106082A8648CE3D03
0107046D306B0201010420F12A1320760270A83CBFFD53F6031EF76A5D86C8A204F2C30CA9EBF51F0F0EA
7A1440342000437CC56D976091E5A723EC7592DFF206EEE7CF9069174D0AD14B5F768225962924EE500D82
311FFEA2FD2345D5D16BD8A88C26B770D55CD8A2A0EFA01C8B4EDFF060606060606"

PBES2
Decrypt (bad, PBKDF2 params explicit prf_alg not a sequence)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_DES_C
mbedtls_pkcs5_pbes2:MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:"301D06092A864886F70D01050C301004082ED7F24A1D516DD702020800310
0":"":"":MBEDTLS_ERR_PKCS5_INVALID_FORMAT + MBEDTLS_ERR_ASN1_UNEXPECTED_TAG:""

PBES2 Decrypt (bad, PBKDF2 params explicit prf_alg overlong)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_DES_C
mbedtls_pkcs5_pbes2:MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:"301D06092A864886F70D01050C301004082ED7F24A1D516DD702020800300
1":"":"":MBEDTLS_ERR_PKCS5_INVALID_FORMAT
+ MBEDTLS_ERR_ASN1_OUT_OF_DATA:""

PBES2 Decrypt (bad, PBKDF2 params explicit prf_alg != HMAC-SHA1)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_DES_C
mbedtls_pkcs5_pbes2:MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:"302706092A864886F70D01050C301A04082ED7F24A1D516DD702020800300
A06082A864886F70D0208":"":"":MBEDTLS_ERR_PKCS5_FEATURE_UNAVAILABLE:""

PBES2 Decrypt (bad, PBKDF2 params extra data)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_DES_C
mbedtls_pkcs5_pbes2:MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:"302806092A864886F70D01050C301B04082ED7F24A1D516DD702020800300
A06082A864886F70D020700":"":"":MBEDTLS_ERR_PKCS5_INVALID_FORMAT +
MBEDTLS_ERR_ASN1_LENGTH_MISMATCH:""

PBES2 Decrypt (bad enc_scheme_alg: not a sequence)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_DES_C
mbedtls_pkcs5_pbes2:MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:"301B06092A864886F70D01050C300E04082ED7F24A1D516DD702020800310
0":"":"":MBEDTLS_ERR_PKCS5_INVALID_FORMAT
+ MBEDTLS_ERR_ASN1_UNEXPECTED_TAG:""

PBES2 Decrypt (bad enc_scheme_alg: overlong)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_DES_C
mbedtls_pkcs5_pbes2:MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:"301B06092A864886F70D01050C300E04082ED7F24A1D516DD702020800300
1":"":"":MBEDTLS_ERR_PKCS5_INVALID_FORMAT + MBEDTLS_ERR_ASN1_OUT_OF_DATA:""

PBES2 Decrypt (bad enc_scheme_alg: unknown oid)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_DES_C
mbedtls_pkcs5_pbes2:MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:"301B06092A864886F70D01050C300E04082ED7F24A1D516DD702020800300
A06082A864886F70D03FF":"":"":MBEDTLS_ERR_PKCS5_FEATURE_UNAVAILABLE:""

PBES2 Decrypt (bad enc_scheme_alg params: not an octet string)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC
mbedtls_pkcs5_pbes2:MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:"301B06092A864886F70D01050C300E04082ED7F24A1D516DD702020800300
C06082A864886F70D03070500":"":"":MBEDTLS_ERR_PKCS5_INVALID_FORMAT:""

PBES2 Decrypt (bad enc_scheme_alg
params: overlong)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_DES_C

mbedtls_pkcs5_pbes2:MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:"301B06092A864886F70D01050C300E04082ED7F24A1D516DD702020800300
C06082A864886F70D03070401":"":"":MBEDTLS_ERR_PKCS5_INVALID_FORMAT +
MBEDTLS_ERR_ASN1_OUT_OF_DATA:""

PBES2 Decrypt (bad enc_scheme_alg params: len != iv_len)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC
mbedtls_pkcs5_pbes2:MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:"301B06092A864886F70D01050C300E04082ED7F24A1D516DD702020800301
306082A864886F70D030704078A4FCC9DCC3949":"":"":MBEDTLS_ERR_PKCS5_INVALID_FORMAT:""

PBES2 Decrypt (bad password)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC
mbedtls_pkcs5_pbes2:MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:"301B06092A864886F70D01050C300E04082ED7F24A1D516DD702020800301
406082A864886F70D030704088A4FCC9DCC394910":"F0617373776f7264":"1B60098D4834CA752D37B430E7
0B7A085CFF86E21F4849F969DD1DF623342662443F8BD1252BF83CEF6917551B08EF55A69C8F2BFFC93BC
B2DFE2E354DA28F896D1BD1BFB972A1251219A6EC7183B0A4CF2C4998449ED786CAE2138437289EB2203
974000C38619DA57A4E685D29649284602BD1806131772DA11A682674DC22B2CF109128DDB7FD980E1C57
41FC0DB7":MBEDTLS_ERR_PKCS5_PASSWORD_MISMATCH:"308187020100301306072A8648CE3D02010
6082A8648CE3D030107046D306B0201010420F12A1320760270A83CBFFD53F6031EF76A5D86C8A204F2C30
CA9EBF51F0F0EA7A1440342000437CC56D976091E5A723EC7592DFF206EEE7CF9069174D0AD14B5F7682
25962924EE500D82311FFEA2FD2345D5D16BD8A88C26B770D55CD8A2A0EFA01C8B4EDFF060606060606"

PBES2
Decrypt (bad iter value)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_DES_C:MBEDTLS_CIPHER_MODE_CBC
mbedtls_pkcs5_pbes2:MBEDTLS_ASN1_CONSTRUCTED |
MBEDTLS_ASN1_SEQUENCE:"301B06092A864886F70D01050C300E04082ED7F24A1D516DD702020801301
406082A864886F70D030704088A4FCC9DCC394910":"70617373776f7264":"1B60098D4834CA752D37B430E7
0B7A085CFF86E21F4849F969DD1DF623342662443F8BD1252BF83CEF6917551B08EF55A69C8F2BFFC93BC
B2DFE2E354DA28F896D1BD1BFB972A1251219A6EC7183B0A4CF2C4998449ED786CAE2138437289EB2203
974000C38619DA57A4E685D29649284602BD1806131772DA11A682674DC22B2CF109128DDB7FD980E1C57
41FC0DB7":MBEDTLS_ERR_PKCS5_PASSWORD_MISMATCH:"308187020100301306072A8648CE3D02010
6082A8648CE3D030107046D306B0201010420F12A1320760270A83CBFFD53F6031EF76A5D86C8A204F2C30
CA9EBF51F0F0EA7A1440342000437CC56D976091E5A723EC7592DFF206EEE7CF9069174D0AD14B5F7682
25962924EE500D82311FFEA2FD2345D5D16BD8A88C26B770D55CD8A2A0EFA01C8B4EDFF060606060606"

PKCS#5
Selftest
pkcs5_selftest:
-----BEGIN CERTIFICATE-----
MIIDDDCCAfSgAwIBAgIBATANBgkqhkiG9w0BAQsFADAmMSQwIgYDVQQDExtUZXN0
IGludGVybWVkaWF0ZSBtYXhwYXRoIDMwHhcNMDEwMTAxMDAwMDAwWhcNMzAxMjMx
MjM1OTU5WjAeMRwwGgYDVQQDExNUZXN0IGxlYWYgaW52YWxpZCA0MIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAkcNsE/s4nauA5vSG/23znHT5ZjFAQiRa
83xo83MD2jMrBjgBBzOW0IKedk9lmqcRmoMsWt3PbYeH2Am+EqtOjh9vbHw/wXEw
eXg7DtZaYTjeRNkrwZ0z5Bz/TTvia7YkcfaU83OG4JyL8GmmbtiGNOHZyHqTv2Ky

j6YqyBJaDE7dwBNBJd5DElEuvr6Tu/Y3K3Z6z8bZUAX/5oII2sq8rg76ZQ+Dfk8i
upjp4MVPvowh/+ys+WNMW5MA5k1dwYyU1MZ20O/aa9VTMkb4DPyv4pXZgi1dBCMc
YskPRVoPPsE5xl3DZ3h4qZ039MbcalXFYe65689+Ra1O4/dsXR5raQIDAQABo00w
SzAJBgNVHRMEAjAAMB0GA1UdDgQWBBTKtXdQZA8cZkS/89eiih4GTJX+fDAfBgNV
HSMEGDAWgBSOBr1U4h5PYyOqGe/gJgwWk7FfezANBgkqhkiG9w0BAQsFAAOCAQEA
IWynyo8ezt+So+w29h7z2ZS3/EcrErnSiDDJ0DaE/vcvflrT/tEPeDHTxy61qQuX
KoseO84foFqLPu1YqgSjRgmbk76gt8aAu0lr6/t0RHWdHKZG3QtK8696pGoMAhVg
Ha3f/YYaEkqSnHwU+/vxEXEkGHM22UHwb7dtH2LfBHtoQtjE6M+Ulv6QdkLj2LFD
XMKJIyAlibTRMW8YOP4G/DekCq1DstUOcTn7BFqeAjjzYwv3NHpOJHdZrUgyGb7B
QqDXf2rM3s7LEpwDMvfdraAEWld4/LRLkfau/PfKD5YwGYg3Nb45xyXFSEijVjAr
23G8HAIcJJu2jUIWGr9OtQ==
-----END
CERTIFICATE-----
-----BEGIN PRIVATE KEY-----
MIICdQIBADANBgkqhkiG9w0BAQEFAASCAl8wggJbAgEAAoGBAMDRSzONESX4mSVT
J69o3x9vQanXcPNviljcwKgkrXkFah6hQUAhW+4jQLxtGb+LU47gE321JGtGNb5L
z1htjLULvc9SAplJ6OOcQUDhyFxI4o6FmUzorv49ytzH6x2IO7UOF44MyJIWGjG3
4fohS8EQaQjkBYW7kwM/vCVT8Bl9AgMBAAECgYBTqj0cSEi5li41kOh2Z2XxiOAQ
J0h+iNaaCmeaThfrnFrYoZXjktYF9cwANsLmZzlBlJ9Ae5oq5hMp2FFHCHn1z1U/
BiE3yF2AXNslL0p8lMO4qGxmt2iYdE3Z8comfkyttUJ5k9thLQzU/NWATP8EZGng
iTdEDFOW35cG26ccDQJBAPPoaiveAVN0JYxe2tYR8xb5qta89QGU6HDdTRiClap1
5rfph5d30MQggqf1tBTiDRKOSk7uN39xwGbMzz11+NcCQQDKYHXWAsN3QlmFQKTX
nm4G5xpl57P9U25wSC+NYOmFEieomD7YlbaBKBc0V5JNj2IqUt0EvXNh3LA5czd9
3pHLAkAioVgZvF6h07bVFE6r4EaMd4xbCt8ah2LtS2570WagmjbU2/JlfhyFDDyg
zlDwOhwzC0LfrBDzJlpz/hZamppnAkBswjIRdSK+sLWTWw47ojTXGNOi+EZOWcv8
I48Kl45nqT4O6OK9WpfeCUGPK5DAhdHnlOiaZ4Xejc9W0Ih96GLJAkBOzJE8nUU5
giUjLAxJoYepKlWh5tZsNDoGFg46+bHn9l1O6fX7tau0+jEz4tC6aA8R3HtUOrYv
hJ61gH8x3U5J
-----END PRIVATE KEY-----
This is just to make sure files that don't parse as certs are ignored.
PK utils: RSA
depends_on:MBEDTLS_RSA_C:MBEDTLS_GENPRIME
pk_utils:MBEDTLS_PK_RSA:512:64:"RSA"

PK utils: ECKEY
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP192R1_ENABLED
pk_utils:MBEDTLS_PK_ECKEY:192:24:"EC"

PK utils: ECKEY_DH
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP192R1_ENABLED
pk_utils:MBEDTLS_PK_ECKEY_DH:192:24:"EC_DH"

PK utils: ECDSA
depends_on:MBEDTLS_ECDSA_C:MBEDTLS_ECP_DP_SECP192R1_ENABLED
pk_utils:MBEDTLS_PK_ECDSA:192:24:"ECDSA"

RSA verify test vector #1 (good)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_PKCS1_V15

pk_rsa_verify_test_vec:"206ef4bf396c6087f8229ef196fd35f37ccb8de5efcdb238f20d556668f114257a11fbe038464a67830378e62ae9791453953dac1dbd7921837ba98e84e856eb80ed9487e656d0b20c28c8ba5e35db1abbed83ed1c7720a97701f709e3547a4bfcabca9c89c57ad15c3996577a0ae36d7c7b699035242f37954646c1cd5c08ac":MBEDTLS_MD_SHA1:1024:16:"e28a13548525e5f36dccb24ecb7cc332cc689dfd64012604c9c7816d72a16c3f5fcdc0e86e7c03280b1c69b586ce0cd8aec722cc73a5d3b730310bf7dfebdc77ce5d94bbc369dc18a2f7b07bd505ab0f82224aef09fdc1e5063234255e0b3c40a52e9e8ae60898eb88a766bdd788fe9493d8fd86bcdd2884d5c06216c65469e5":16:"3":"5abc01f5de25b70867ff0c24e222c61f53c88daf42586fddcd56f3c4588f074be3c328056c063388688b6385a8167957c6e5355a510e005b8a851d69c96b36ec6036644078210e5d7d326f96365ee0648882921492bc7b753eb9c26cdbab37555f210df2ca6fec1b25b463d38b81c0dcea202022b04af5da58aa03d77be949b7":0

RSA
 verify test vector #2 (bad)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_PKCS1_V15
pk_rsa_verify_test_vec:"d6248c3e96b1a7e5fea978870fcc4c9786b4e5156e16b7faef4557d667f730b8bc4c784ef00c624df5309513c3a5de8ca94c2152e0459618666d3148092562ebc256ffca45b27fd2d63c68bd5e0a0aefbe496e9e63838a361b1db6fc272464f191490bf9c029643c49d2d9cd08833b8a70b4b3431f56fb1eb55ccd39e77a9c92":MBEDTLS_MD_SHA1:1024:16:"e28a13548525e5f36dccb24ecb7cc332cc689dfd64012604c9c7816d72a16c3f5fcdc0e86e7c03280b1c69b586ce0cd8aec722cc73a5d3b730310bf7dfebdc77ce5d94bbc369dc18a2f7b07bd505ab0f82224aef09fdc1e5063234255e0b3c40a52e9e8ae60898eb88a766bdd788fe9493d8fd86bcdd2884d5c06216c65469e5":16:"3":"3203b7647fb7e345aa457681e5131777f1adc371f2fba8534928c4e52ef6206a856425d6269352ecbf64db2f6ad82397768cafdd8cd272e512d617ad67992226da6bc291c31404c17fd4b7e2beb20eff284a44f4d7af47fd6629e2c95809fa7f2241a04f70ac70d3271bb13258af1ed5c5988c95df7fa26603515791075feccd":MBEDTLS_ERR_RSA_VERIFY_FAILED

ECDSA
 verify test vector #1 (good)
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
pk_ec_test_vec:MBEDTLS_PK_ECDSA:MBEDTLS_ECP_DP_SECP192R1:"046FDD3028FA94A863CD4F78DBFF8B3AA561FC6D9CCBBCA88E0AE6FA437F5415F957542D0717FF8B84562DAE99872EF841":"546869732073686F756C6420626520746865206861736820617368206F662061206D6573736167652E00":"30350218185B2A7FB5CD9C9A8488B119B68B47D6EC833509CE9FA1FF021900FB7D259A744A2348BD45D241A39DC915B81CC2084100FA24":0

ECDSA verify test vector #2 (bad)
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
pk_ec_test_vec:MBEDTLS_PK_ECDSA:MBEDTLS_ECP_DP_SECP192R1:"046FDD3028FA94A863CD4F78DBFF8B3AA561FC6D9CCBBCA88E0AE6FA437F5415F957542D0717FF8B84562DAE99872EF841":"546869732073686F756C6420626520746865206861736820617368206F662061206D6573736167652E00":"30350218185B2A7FB5CD9C9A8488B119B68B47D6EC833509CE9FA1FF021900FB7D259A744A2348BD45D241A39DC915B81CC2084100FA25":MBEDTLS_ERR_ECP_VERIFY_FAILED

EC(DSA)
 verify test vector #1 (good)
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
pk_ec_test_vec:MBEDTLS_PK_ECKEY:MBEDTLS_ECP_DP_SECP192R1:"046FDD3028FA94A863CD4F78DBFF8B3AA561FC6D9CCBBCA88E0AE6FA437F5415F957542D0717FF8B84562DAE99872EF841":"546869732073686F756C6420626520746865206861736820617368206F662061206D6573736167652E00":"30350218185B2A7FB5CD9C9A8488B119B68B47D6EC833509CE9FA1FF021900FB7D259A744A2348BD45D241A39DC915B81CC2084100FA24":0

EC(DSA) verify test vector #2 (bad)
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
pk_ec_test_vec:MBEDTLS_PK_ECKEY:MBEDTLS_ECP_DP_SECP192R1:"046FDD3028FA94A863CD4F78D
BFF8B3AA561FC6D9CCBBCA88E0AE6FA437F5415F957542D0717FF8B84562DAE99872EF841":"546869732
073686F756C6420626520746865206861736820 6F662061206D6573736167652E00":"30350218185B2A7FB5CD9
C9A8488B119B68B47D6EC833509CE9FA1FF021900FB7D259A744A2348BD45D241A39DC915B81CC208410
0FA25":MBEDTLS_ERR_ECP_VERIFY_FAILED

ECDSA
sign-verify
depends_on:MBEDTLS_ECDSA_C:MBEDTLS_ECP_DP_SECP192R1_ENABLED
pk_sign_verify:MBEDTLS_PK_ECDSA:0:0

EC(DSA) sign-verify
depends_on:MBEDTLS_ECDSA_C:MBEDTLS_ECP_DP_SECP192R1_ENABLED
pk_sign_verify:MBEDTLS_PK_ECKEY:0:0

EC_DH (no) sign-verify
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP192R1_ENABLED
pk_sign_verify:MBEDTLS_PK_ECKEY_DH:MBEDTLS_ERR_PK_TYPE_MISMATCH:MBEDTLS_ERR_PK_
TYPE_MISMATCH

RSA sign-verify
depends_on:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15:MBEDTLS_GENPRIME
pk_sign_verify:MBEDTLS_PK_RSA:0:0

RSA encrypt test vector
depends_on:MBEDTLS_PKCS1_V15
pk_rsa_encrypt_test_vec:"4E636AF98E40F3ADCFCCB698F4E80B9F":2048:16:"b38ac65c8141f7f5c96e14470e85
1936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a8417b62675fdc6df46b94813bc7b976
9a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61dc45434c6b54e2c3ee0fc07908509
d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59559dd1d54c9b24190965eafbdab2
03b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543d391ce0adab5351f97a3810c1f73d
7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f35549141486c3b0961a7b4c1a2034
f":16:"3":"b0c0b193ba4a5b4502bfacd1a9c2697da5510f3e3ab7274cf404418afd2c62c89b98d83bbc21c8c1bf1afe6d8
bf40425e053e9c03e03a3be0edbe1eda073fade1cc286cc0305a493d98fe795634c3cad7feb513edb742d66d910c87d07
f6b0055c3488bb262b5fd1ce8747af64801fb39d2d3a3e57086ffe55ab8d0a2ca86975629a0f85767a4990c532a7c2dab
1647997ebb234d0b28a0008bfebfc905e7ba5b30b60566a5e0190417465efdbf549934b8f0c5c9f36b7c5b6373a47ae55
3ced0608a161b1b70dfa509375cf7a3598223a6d7b7a1d1a06ac74d345a9bb7c0e44c8388858a4f1d8115f2bd769ffa69
020385fa286302c80e950f9e2751308666c":0

RSA
decrypt test vector #1
depends_on:MBEDTLS_PKCS1_V15
pk_rsa_decrypt_test_vec:"a42eda41e56235e666e7faaa77100197f657288a1bf183e4820f0c37ce2c456b960278d6003
e0bbcd4be4a969f8e8fd9231e1f492414f00ed09844994c86ec32db7cde3bec7f0c3dbf6ae55baeb2712fa609f5fc3207a8
24eb3dace31849cd6a6084318523912bccb84cf42e3c6d6d1685131d69bb545acec827d2b0dfdd5568b7dcc4f5a11d69

16583fefa689d367f8c9e1d95dcd2240895a9470b0c1730f97cd6e8546860bd254801769f54be96e16362ddcbf34d560
35028890199e0f48db38642cb66a4181e028a6443a404fea284ce02b4614b683367d40874e505611d23142d49f06feea
831d52d347b13610b413c4efc43a6de9f0b08d2a951dc503b6":2048:16:"e79a373182bfaa722eb035f772ad2a9464bd8
42de59432c18bbab3a7dfeae318c9b915ee487861ab665a40bd6cda560152578e8579016c929df99fea05b4d64efca1d5
43850bc8164b40d71ed7f3fa4105df0fb9b9ad2a18ce182c8a4f4f975bea9aa0b9a1438a27a28e97ac8330ef37383414d1
bd64607d6979ac050424fd17":16:"c6749cbb0db8c5a177672d4728a8b22392b2fc4d3b8361d5c0d5055a1b4e46d821f
757c24eef2a51c561941b93b3ace7340074c058c9bb48e7e7414f42c41da4cccb5c2ba91deb30c586b7fb18af12a52995
592ad139d3be429add6547e044becedaf31fa3b39421e24ee034fbf367d11f6b8f88ee483d163b431e1654ad3e89":16:"
b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a841
7b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61d
c45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59
559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543
d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f3
5549141486c3b0961a7b4c1a2034f":16:"3":"4E636AF98E40F3ADCFCCB698F4E80B9F":0

RSA
 decrypt test vector #2
depends_on:MBEDTLS_PKCS1_V15
pk_rsa_decrypt_test_vec:"a42eda41e56235e666e7faaa77100197f657288a1bf183e4820f0c37ce2c456b960278d6003
e0bbcd4be4a969f8e8fd9231e1f492414f00ed09844994c86ec32db7cde3bec7f0c3dbf6ae55baeb2712fa609f5fc3207a8
24eb3dace31849cd6a6084318523912bccb84cf42e3c6d6d1685131d69bb545acec827d2b0dfdd5568b7dcc4f5a11d69
16583fefa689d367f8c9e1d95dcd2240895a9470b0c1730f97cd6e8546860bd254801769f54be96e16362ddcbf34d560
35028890199e0f48db38642cb66a4181e028a6443a404feb284ce02b4614b683367d40874e505611d23142d49f06feea
831d52d347b13610b413c4efc43a6de9f0b08d2a951dc503b6":2048:16:"e79a373182bfaa722eb035f772ad2a9464bd8
42de59432c18bbab3a7dfeae318c9b915ee487861ab665a40bd6cda560152578e8579016c929df99fea05b4d64efca1d5
43850bc8164b40d71ed7f3fa4105df0fb9b9ad2a18ce182c8a4f4f975bea9aa0b9a1438a27a28e97ac8330ef37383414d1
bd64607d6979ac050424fd17":16:"c6749cbb0db8c5a177672d4728a8b22392b2fc4d3b8361d5c0d5055a1b4e46d821f
757c24eef2a51c561941b93b3ace7340074c058c9bb48e7e7414f42c41da4cccb5c2ba91deb30c586b7fb18af12a52995
592ad139d3be429add6547e044becedaf31fa3b39421e24ee034fbf367d11f6b8f88ee483d163b431e1654ad3e89":16:"
b38ac65c8141f7f5c96e14470e851936a67bf94cc6821a39ac12c05f7c0b06d9e6ddba2224703b02e25f31452f9c4a841
7b62675fdc6df46b94813bc7b9769a892c482b830bfe0ad42e46668ace68903617faf6681f4babf1cc8e4b0420d3c7f61d
c45434c6b54e2c3ee0fc07908509d79c9826e673bf8363255adb0add2401039a7bcd1b4ecf0fbe6ec8369d2da486eec59
559dd1d54c9b24190965eafbdab203b35255765261cd0909acf93c3b8b8428cbb448de4715d1b813d0c94829c229543
d391ce0adab5351f97a3810c1f73d7b1458b97daed4209c50e16d064d2d5bfda8c23893d755222793146d0a78c3d64f3
5549141486c3b0961a7b4c1a2034f":16:"3":"4E636AF98E40F3ADCFCCB698F4E80B9F":MBEDTLS_ERR_RSA
_INVALID_PADDING

EC
 nocrypt
depends_on:MBEDTLS_ECP_C
pk_ec_nocrypt:MBEDTLS_PK_ECKEY

EC-DH nocrypt
depends_on:MBEDTLS_ECP_C
pk_ec_nocrypt:MBEDTLS_PK_ECKEY_DH

ECDSA nocrypt
depends_on:MBEDTLS_ECDSA_C

pk_ec_nocrypt:MBEDTLS_PK_ECDSA

RSA_ALT consistency
depends_on:MBEDTLS_RSA_C:MBEDTLS_PKCS1_V15:MBEDTLS_GENPRIME
pk_rsa_alt:

Verify ext RSA #1 (PKCS1 v2.1, salt_len = ANY, OK)
depends_on:MBEDTLS_PKCS1_V21:MBEDTLS_SHA256_C
pk_rsa_verify_ext_test_vec:"54657374206d657373616765":MBEDTLS_MD_SHA256:1024:16:"00dd118a9f99bab
068ca2aea3b6a6d5997ed4ec954e40deecea07da01eaae80ec2bb1340db8a128e891324a5c5f5fad8f590d7c8cacbc5fe9
31dafda1223735279461abaa0572b761631b3a8afe7389b088b63993a0a25ee45d21858bab9931aedd4589a631b37fcf
714089f856549f359326dd1e0e86dde52ed66b4a90bda4095":16:"010001":"0d2bdb0456a3d651d5bd48a4204493898
f72cf1aaddd71387cc058bc3f4c235ea6be4010fd61b28e1fbb275462b53775c04be9022d38b6a2e0387dddba86a3f855
4d2858044a59fddbd594753fc056fe33c8daddb85dc70d164690b1182209ff84824e0be10e35c379f2f378bf176a9f7cb
94d95e44d90276a298c8810f741c9":MBEDTLS_PK_RSASSA_PSS:MBEDTLS_MD_SHA256:MBEDTLS_RSA_
SALT_LEN_ANY:0

Verify
ext RSA #2 (PKCS1 v2.1, salt_len = ANY, wrong message)
depends_on:MBEDTLS_PKCS1_V21:MBEDTLS_SHA256_C
pk_rsa_verify_ext_test_vec:"54657374206d657373616766":MBEDTLS_MD_SHA256:1024:16:"00dd118a9f99bab
068ca2aea3b6a6d5997ed4ec954e40deecea07da01eaae80ec2bb1340db8a128e891324a5c5f5fad8f590d7c8cacbc5fe9
31dafda1223735279461abaa0572b761631b3a8afe7389b088b63993a0a25ee45d21858bab9931aedd4589a631b37fcf
714089f856549f359326dd1e0e86dde52ed66b4a90bda4095":16:"010001":"0d2bdb0456a3d651d5bd48a4204493898
f72cf1aaddd71387cc058bc3f4c235ea6be4010fd61b28e1fbb275462b53775c04be9022d38b6a2e0387dddba86a3f855
4d2858044a59fddbd594753fc056fe33c8daddb85dc70d164690b1182209ff84824e0be10e35c379f2f378bf176a9f7cb
94d95e44d90276a298c8810f741c9":MBEDTLS_PK_RSASSA_PSS:MBEDTLS_MD_SHA256:MBEDTLS_RSA_
SALT_LEN_ANY:MBEDTLS_ERR_RSA_VERIFY_FAILED

Verify
ext RSA #3 (PKCS1 v2.1, salt_len = 0, OK)
depends_on:MBEDTLS_PKCS1_V21:MBEDTLS_SHA256_C
pk_rsa_verify_ext_test_vec:"54657374206d657373616765":MBEDTLS_MD_SHA256:1024:16:"00dd118a9f99bab
068ca2aea3b6a6d5997ed4ec954e40deecea07da01eaae80ec2bb1340db8a128e891324a5c5f5fad8f590d7c8cacbc5fe9
31dafda1223735279461abaa0572b761631b3a8afe7389b088b63993a0a25ee45d21858bab9931aedd4589a631b37fcf
714089f856549f359326dd1e0e86dde52ed66b4a90bda4095":16:"010001":"7fc506d26ca3b22922a1ce39faaedd2731
61b82d9443c56f1a034f131ae4a18cae1474271cb4b66a17d9707ca58b0bdbd3c406b7e65bbcc9bbbce94dc45de807b4
989b23b3e4db74ca29298137837eb90cc83d3219249bc7d480fceaf075203a86e54c4ecfa4e312e39f8f69d76534089a3
6ed9049ca9cfd5ab1db1fa75fe5c8":MBEDTLS_PK_RSASSA_PSS:MBEDTLS_MD_SHA256:0:0

Verify ext RSA #4 (PKCS1 v2.1, salt_len = max, OK)
depends_on:MBEDTLS_PKCS1_V21:MBEDTLS_SHA256_C
pk_rsa_verify_ext_test_vec:"54657374206d657373616765":MBEDTLS_MD_SHA256:1024:16:"00dd118a9f99bab
068ca2aea3b6a6d5997ed4ec954e40deecea07da01eaae80ec2bb1340db8a128e891324a5c5f5fad8f590d7c8cacbc5fe9
31dafda1223735279461abaa0572b761631b3a8afe7389b088b63993a0a25ee45d21858bab9931aedd4589a631b37fcf
714089f856549f359326dd1e0e86dde52ed66b4a90bda4095":16:"010001":"0d2bdb0456a3d651d5bd48a4204493898
f72cf1aaddd71387cc058bc3f4c235ea6be4010fd61b28e1fbb275462b53775c04be9022d38b6a2e0387dddba86a3f855
4d2858044a59fddbd594753fc056fe33c8daddb85dc70d164690b1182209ff84824e0be10e35c379f2f378bf176a9f7cb

94d95e44d90276a298c8810f741c9":MBEDTLS_PK_RSASSA_PSS:MBEDTLS_MD_SHA256:94:0

Verify
ext RSA #5 (PKCS1 v2.1, wrong salt_len)
depends_on:MBEDTLS_PKCS1_V21:MBEDTLS_SHA256_C
pk_rsa_verify_ext_test_vec:"54657374206d657373616765":MBEDTLS_MD_SHA256:1024:16:"00dd118a9f99bab
068ca2aea3b6a6d5997ed4ec954e40deecea07da01eaae80ec2bb1340db8a128e891324a5c5f5fad8f590d7c8cacbc5fe9
31dafda1223735279461abaa0572b761631b3a8afe7389b088b63993a0a25ee45d21858bab9931aedd4589a631b37fcf
714089f856549f359326dd1e0e86dde52ed66b4a90bda4095":16:"010001":"0d2bdb0456a3d651d5bd48a4204493898
f72cf1aaddd71387cc058bc3f4c235ea6be4010fd61b28e1fbb275462b53775c04be9022d38b6a2e0387dddba86a3f855
4d2858044a59fddbd594753fc056fe33c8daddb85dc70d164690b1182209ff84824e0be10e35c379f2f378bf176a9f7cb
94d95e44d90276a298c8810f741c9":MBEDTLS_PK_RSASSA_PSS:MBEDTLS_MD_SHA256:32:MBEDTLS_ER
R_RSA_INVALID_PADDING

Verify
ext RSA #6 (PKCS1 v2.1, MGF1 alg != MSG hash alg)
depends_on:MBEDTLS_PKCS1_V21:MBEDTLS_SHA256_C
pk_rsa_verify_ext_test_vec:"c0719e9a8d5d838d861dc6f675c899d2b309a3a65bb9fe6b11e5afcbf9a2c0b1":MBEDT
LS_MD_NONE:1024:16:"00dd118a9f99bab068ca2aea3b6a6d5997ed4ec954e40deecea07da01eaae80ec2bb1340db8
a128e891324a5c5f5fad8f590d7c8cacbc5fe931dafda1223735279461abaa0572b761631b3a8afe7389b088b63993a0a
25ee45d21858bab9931aedd4589a631b37fcf714089f856549f359326dd1e0e86dde52ed66b4a90bda4095":16:"01000
1":"0d2bdb0456a3d651d5bd48a4204493898f72cf1aaddd71387cc058bc3f4c235ea6be4010fd61b28e1fbb275462b53
775c04be9022d38b6a2e0387dddba86a3f8554d2858044a59fddbd594753fc056fe33c8daddb85dc70d164690b118220
9ff84824e0be10e35c379f2f378bf176a9f7cb94d95e44d90276a298c8810f741c9":MBEDTLS_PK_RSASSA_PSS:M
BEDTLS_MD_SHA256:MBEDTLS_RSA_SALT_LEN_ANY:0

Verify
ext RSA #7 (PKCS1 v2.1, wrong MGF1 alg != MSG hash alg)
depends_on:MBEDTLS_PKCS1_V21:MBEDTLS_SHA256_C:MBEDTLS_SHA1_C
pk_rsa_verify_ext_test_vec:"c0719e9a8d5d838d861dc6f675c899d2b309a3a65bb9fe6b11e5afcbf9a2c0b1":MBEDT
LS_MD_NONE:1024:16:"00dd118a9f99bab068ca2aea3b6a6d5997ed4ec954e40deecea07da01eaae80ec2bb1340db8
a128e891324a5c5f5fad8f590d7c8cacbc5fe931dafda1223735279461abaa0572b761631b3a8afe7389b088b63993a0a
25ee45d21858bab9931aedd4589a631b37fcf714089f856549f359326dd1e0e86dde52ed66b4a90bda4095":16:"01000
1":"0d2bdb0456a3d651d5bd48a4204493898f72cf1aaddd71387cc058bc3f4c235ea6be4010fd61b28e1fbb275462b53
775c04be9022d38b6a2e0387dddba86a3f8554d2858044a59fddbd594753fc056fe33c8daddb85dc70d164690b118220
9ff84824e0be10e35c379f2f378bf176a9f7cb94d95e44d90276a298c8810f741c9":MBEDTLS_PK_RSASSA_PSS:M
BEDTLS_MD_SHA1:MBEDTLS_RSA_SALT_LEN_ANY:MBEDTLS_ERR_RSA_INVALID_PADDING

Verify
ext RSA #8 (PKCS1 v2.1, RSASSA-PSS without options)
depends_on:MBEDTLS_PKCS1_V21:MBEDTLS_SHA256_C
pk_rsa_verify_ext_test_vec:"54657374206d657373616765":MBEDTLS_MD_SHA256:1024:16:"00dd118a9f99bab
068ca2aea3b6a6d5997ed4ec954e40deecea07da01eaae80ec2bb1340db8a128e891324a5c5f5fad8f590d7c8cacbc5fe9
31dafda1223735279461abaa0572b761631b3a8afe7389b088b63993a0a25ee45d21858bab9931aedd4589a631b37fcf
714089f856549f359326dd1e0e86dde52ed66b4a90bda4095":16:"010001":"0d2bdb0456a3d651d5bd48a4204493898
f72cf1aaddd71387cc058bc3f4c235ea6be4010fd61b28e1fbb275462b53775c04be9022d38b6a2e0387dddba86a3f855
4d2858044a59fddbd594753fc056fe33c8daddb85dc70d164690b1182209ff84824e0be10e35c379f2f378bf176a9f7cb
94d95e44d90276a298c8810f741c9":MBEDTLS_PK_RSASSA_PSS:-

1:MBEDTLS_RSA_SALT_LEN_ANY:MBEDTLS_ERR_PK_BAD_INPUT_DATA

Verify ext RSA #9 (PKCS1 v2.1, RSA with options)
depends_on:MBEDTLS_PKCS1_V15:MBEDTLS_SHA256_C
pk_rsa_verify_ext_test_vec:"54657374206d657373616765":MBEDTLS_MD_SHA256:1024:16:"00dd118a9f99bab
068ca2aea3b6a6d5997ed4ec954e40deecea07da01eaae80ec2bb1340db8a128e891324a5c5f5fad8f590d7c8cacbc5fe9
31dafda1223735279461abaa0572b761631b3a8afe7389b088b63993a0a25ee45d21858bab9931aedd4589a631b37fcf
714089f856549f359326dd1e0e86dde52ed66b4a90bda4095":16:"010001":"0d2bdb0456a3d651d5bd48a4204493898
f72cf1aaddd71387cc058bc3f4c235ea6be4010fd61b28e1fbb275462b53775c04be9022d38b6a2e0387dddba86a3f855
4d2858044a59fddbd594753fc056fe33c8daddb85dc70d164690b1182209ff84824e0be10e35c379f2f378bf176a9f7cb
94d95e44d90276a298c8810f741c9":MBEDTLS_PK_RSA:MBEDTLS_MD_SHA256:MBEDTLS_RSA_SALT_L
EN_ANY:MBEDTLS_ERR_PK_BAD_INPUT_DATA

Verify
ext RSA #10 (PKCS1 v2.1, RSA without options)
depends_on:MBEDTLS_PKCS1_V15:MBEDTLS_SHA256_C
pk_rsa_verify_ext_test_vec:"54657374206d657373616765":MBEDTLS_MD_SHA256:1024:16:"00dd118a9f99bab
068ca2aea3b6a6d5997ed4ec954e40deecea07da01eaae80ec2bb1340db8a128e891324a5c5f5fad8f590d7c8cacbc5fe9
31dafda1223735279461abaa0572b761631b3a8afe7389b088b63993a0a25ee45d21858bab9931aedd4589a631b37fcf
714089f856549f359326dd1e0e86dde52ed66b4a90bda4095":16:"010001":"0d2bdb0456a3d651d5bd48a4204493898
f72cf1aaddd71387cc058bc3f4c235ea6be4010fd61b28e1fbb275462b53775c04be9022d38b6a2e0387dddba86a3f855
4d2858044a59fddbd594753fc056fe33c8daddb85dc70d164690b1182209ff84824e0be10e35c379f2f378bf176a9f7cb
94d95e44d90276a298c8810f741c9":MBEDTLS_PK_RSA:-
1:MBEDTLS_RSA_SALT_LEN_ANY:MBEDTLS_ERR_RSA_INVALID_PADDING

Verify
ext RSA #11 (PKCS1 v2.1, asking for ECDSA)
depends_on:MBEDTLS_ECDSA_C:MBEDTLS_SHA256_C
pk_rsa_verify_ext_test_vec:"54657374206d657373616765":MBEDTLS_MD_SHA256:1024:16:"00dd118a9f99bab
068ca2aea3b6a6d5997ed4ec954e40deecea07da01eaae80ec2bb1340db8a128e891324a5c5f5fad8f590d7c8cacbc5fe9
31dafda1223735279461abaa0572b761631b3a8afe7389b088b63993a0a25ee45d21858bab9931aedd4589a631b37fcf
714089f856549f359326dd1e0e86dde52ed66b4a90bda4095":16:"010001":"0d2bdb0456a3d651d5bd48a4204493898
f72cf1aaddd71387cc058bc3f4c235ea6be4010fd61b28e1fbb275462b53775c04be9022d38b6a2e0387dddba86a3f855
4d2858044a59fddbd594753fc056fe33c8daddb85dc70d164690b1182209ff84824e0be10e35c379f2f378bf176a9f7cb
94d95e44d90276a298c8810f741c9":MBEDTLS_PK_ECDSA:-
1:MBEDTLS_RSA_SALT_LEN_ANY:MBEDTLS_ERR_PK_TYPE_MISMATCH

Verify
ext RSA #12 (PKCS1 v1.5, good)
depends_on:MBEDTLS_SHA1_C:MBEDTLS_PKCS1_V15
pk_rsa_verify_ext_test_vec:"206ef4bf396c6087f8229ef196fd35f37ccb8de5efcdb238f20d556668f114257a11fbe038
464a67830378e62ae9791453953dac1dbd7921837ba98e84e856eb80ed9487e656d0b20c28c8ba5e35db1abbed83ed1
c7720a97701f709e3547a4bfcabca9c89c57ad15c3996577a0ae36d7c7b699035242f37954646c1cd5c08ac":MBEDTL
S_MD_SHA1:1024:16:"e28a13548525e5f36dccb24ecb7cc332cc689dfd64012604c9c7816d72a16c3f5fcdc0e86e7c0
3280b1c69b586ce0cd8aec722cc73a5d3b730310bf7dfebdc77ce5d94bbc369dc18a2f7b07bd505ab0f82224aef09fdc1e
5063234255e0b3c40a52e9e8ae60898eb88a766bdd788fe9493d8fd86bcdd2884d5c06216c65469e5":16:"3":"5abc01f
5de25b70867ff0c24e222c61f53c88daf42586fddcd56f3c4588f074be3c328056c063388688b6385a8167957c6e5355a
510e005b8a851d69c96b36ec6036644078210e5d7d326f96365ee0648882921492bc7b753eb9c26cdbab37555f210df2

ca6fec1b25b463d38b81c0dcea202022b04af5da58aa03d77be949b7":MBEDTLS_PK_RSA:-1:MBEDTLS_RSA_SALT_LEN_ANY:0

Check
pair #1 (EC, OK)
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED
mbedtls_pk_check_pair:"data_files/ec_256_pub.pem":"data_files/ec_256_prv.pem":0

Check pair #2 (EC, bad)
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED
mbedtls_pk_check_pair:"data_files/ec_256_pub.pem":"data_files/server5.key":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

Check pair #3 (RSA, OK)
depends_on:MBEDTLS_RSA_C
mbedtls_pk_check_pair:"data_files/server1.pubkey":"data_files/server1.key":0

Check pair #4 (RSA, bad)
depends_on:MBEDTLS_RSA_C
mbedtls_pk_check_pair:"data_files/server1.pubkey":"data_files/server2.key":MBEDTLS_ERR_RSA_KEY_CHECK_FAILED

Check pair #5 (RSA vs EC)
depends_on:MBEDTLS_ECP_C:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_RSA_C
mbedtls_pk_check_pair:"data_files/ec_256_pub.pem":"data_files/server1.key":MBEDTLS_ERR_PK_TYPE_MISMATCH

RSA
hash_len overflow (size_t vs unsigned int)
depends_on:MBEDTLS_RSA_C:MBEDTLS_HAVE_INT64
pk_rsa_overflow:
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">

```
    <Configuration>Release</Configuration>
    <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\test\selftest.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">

  <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid>{7DBC5F77-3DA1-5F73-8421-E693D95FC66A}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>selftest</RootNamespace>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
```

```
 />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
   <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
    <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
   <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <LinkIncremental>false</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
   <LinkIncremental>false</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <ClCompile>
     <PrecompiledHeader>
     </PrecompiledHeader>
     <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
      <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
     <SubSystem>Console</SubSystem>
     <GenerateDebugInformation>true</GenerateDebugInformation>
     <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
     <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
```

```
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
  </Link>
```

```
 </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
   <ClCompile>
     <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
     </PrecompiledHeader>
     <Optimization>MaxSpeed</Optimization>
     <FunctionLevelLinking>true</FunctionLevelLinking>
     <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
   <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
     <SubSystem>Console</SubSystem>
     <GenerateDebugInformation>true</GenerateDebugInformation>
     <EnableCOMDATFolding>true</EnableCOMDATFolding>
     <OptimizeReferences>true</OptimizeReferences>
     <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
     <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
   </Link>
 </ItemDefinitionGroup>
 <Import
 Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
0A0*H=*H='0% Hm4'_*
O7
Certificate:
   Data:
       Version: 3 (0x2)
       Serial Number: 2 (0x2)
       Signature Algorithm: sha1WithRSAEncryption
       Issuer: C=NL, O=PolarSSL, CN=PolarSSL Test CA
       Validity
          Not Before: Feb 12 14:44:06 2011 GMT
          Not After : Feb 12 14:44:06 2021 GMT
       Subject: C=NL, O=PolarSSL, CN=localhost
       Subject Public Key Info:
          Public Key Algorithm: rsaEncryption
          RSA Public Key: (2048 bit)
             Modulus (2048 bit):
                00:c1:4d:a3:dd:e7:cd:1d:d1:04:d7:49:72:b8:99:
                ac:0e:78:e4:3a:3c:4a:cf:3a:13:16:d0:5a:e4:cd:
                a3:00:88:a7:ee:1e:6b:96:a7:52:b4:90:ef:2d:72:
                7a:3e:24:9a:fc:b6:34:ac:24:f5:77:e0:26:64:8c:
                9c:b0:28:7d:a1:da:ea:8c:e6:c9:1c:96:bc:fe:c1:
                04:52:b3:36:d4:a3:fa:e1:b1:76:d8:90:c1:61:b4:
```

66:52:36:a2:26:53:aa:ab:74:5e:07:7d:19:82:db:
2a:d8:1f:a0:d9:0d:1c:2d:49:66:f7:5b:25:73:46:
e8:0b:8a:4f:69:0c:b5:00:90:e1:da:82:10:66:7d:
ae:54:2b:8b:65:79:91:a1:e2:61:c3:cd:40:49:08:
ee:68:0c:f1:8b:86:d2:46:bf:d0:b8:aa:11:03:1e:
7f:56:a8:1a:1e:44:18:0f:0f:85:8b:da:8b:44:5e:
e2:18:c6:62:2f:c7:66:8d:fa:5d:d8:7d:f3:27:89:
29:01:c5:90:0e:3f:27:f1:30:c8:4a:0e:ef:d6:de:
c7:c7:27:6b:c7:05:3d:7a:c4:02:3c:9a:1d:3e:0f:
e8:34:98:5b:cb:73:4b:52:96:d8:11:a2:2c:80:88:
69:39:5a:d3:0f:b0:de:59:2f:11:c7:f7:ea:12:01:
30:97
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
X509v3 Subject Key Identifier:
A5:05:E8:64:B8:DC:DF:60:0F:50:12:4D:60:A8:64:AF:4D:8B:43:93
X509v3 Authority Key Identifier:
keyid:B4:5A:E4:A5:B3:DE:D2:52:F6:B9:D5:A6:95:0F:EB:3E:BC:C7:FD:FF

Signature Algorithm: sha1WithRSAEncryption
9c:67:5c:29:58:a0:79:1b:a7:bd:1c:a8:1a:ec:19:72:f2:6c:
0e:f8:73:36:ce:e5:17:4b:12:01:6c:ee:b1:d5:4b:da:fe:73:
6f:77:96:e4:bf:29:d9:62:2d:27:19:a8:0c:d8:57:29:70:51:
f4:56:bc:a3:28:5a:11:d8:2a:9d:dd:10:84:b8:c5:35:e4:eb:
fe:73:5f:18:6f:f5:1c:3c:48:67:3c:aa:7e:af:21:31:e4:d5:
2d:66:3d:eb:ed:7a:48:1a:b1:8e:58:89:64:2e:33:78:78:61:
59:51:1f:71:c7:10:c0:03:d5:39:c0:7b:17:d7:1c:70:c5:40:
67:be:05:dd:62:01:bc:f5:fe:c1:fd:1f:c9:78:4a:dc:17:e9:
e8:2f:4c:ad:cc:c1:74:70:90:a9:2f:8c:a6:84:0c:0f:40:4d:
b6:71:d2:62:3c:2c:6b:31:4a:e0:aa:7b:da:fd:77:28:e6:b6:
d7:78:ec:9d:69:d5:1b:a5:cf:70:8b:cd:a4:5c:54:8b:92:45:
14:1f:68:3f:27:78:cf:5c:d5:2f:e2:27:f6:a6:4d:5a:89:c4:
0d:4a:39:d3:92:e7:bf:34:5a:13:df:48:0a:c0:fa:0e:2a:02:
64:a3:7a:57:37:a7:8c:16:a6:16:bc:ce:1b:98:c2:35:6e:5f:
a2:47:1b:47
-----BEGIN CERTIFICATE-----
MIIDNzCCAh+gAwIBAgIBAjANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTEwMjEyMTQ0NDA2WhcNMjEwMjEyMTQ0NDA2WjA0MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxEjAQBgNVBAMTCWxvY2FsaG9zdDCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBAMFNo93nzR3RBNdJcriZrA545Do8Ss86ExbQWuTN
owCIp+4ea5anUrSQ7y1yej4kmvy2NKwk9XfgJmSMnLAofaHa6ozmyRyWvP7BBFKz
NtSj+uGxdtiQwWG0ZlI2oiZTqqt0Xgd9GYLbKtgfoNkNHC1JZvdbJXNG6AuKT2kM
tQCQ4dqCEGZ9rlQri2V5kaHiYcPNQEkI7mgM8YuG0ka/0LiqEQMef1aoGh5EGA8P
hYvai0Re4hjGYi/HZo36Xdh98yeJKQHFkA4/J/EwyEoO79bex8cna8cFPXrEAjya
HT4P6DSYW8tzS1KW2BGiLICIaTla0w+w3lkvEcf36hIBMJcCAwEAAaNNMEswCQYD

VR0TBAIwADAdBgNVHQ4EFgQUpQXoZLjc32APUBJNYKhkr02LQ5MwHwYDVR0jBBgw
FoAUtFrkpbPe0lL2udWmlQ/rPrzH/f8wDQYJKoZIhvcNAQEFBQADggEBAJxnXClY
oHkbp70cqBrsGXLybA74czbO5RdLEgFs7rHVS9r+c293luS/KdliLScZqAzYVylw
UfRWvKMoWhHYKp3dEIS4xTXk6/5zXxhv9Rw8SGc8qn6vITHk1S1mPevtekgasY5Y
iWQuM3h4YVlRH3HHEMAD1TnAexfXHHDFQGe+Bd1iAbz1/sH9H8l4StwX6egvTK3M
wXRwkKkvjKaEDA9ATbZx0mI8LGsxSuCqe9r9dyjmttd47J1p1Rulz3CLzaRcVIuS
RRQfaD8neM9c1S/iJ/amTVqJxA1KOdOS5780WhPfSArA+g4qAmSjelc3p4wWpha8
zhuYwjVuX6JHG0c=
-----END
CERTIFICATE-----
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
<ItemGroup Label="ProjectConfigurations">
<ProjectConfiguration Include="Debug|Win32">
<Configuration>Debug</Configuration>
<Platform>Win32</Platform>
</ProjectConfiguration>
<ProjectConfiguration Include="Debug|x64">
<Configuration>Debug</Configuration>
<Platform>x64</Platform>
</ProjectConfiguration>
<ProjectConfiguration Include="Release|Win32">
<Configuration>Release</Configuration>
<Platform>Win32</Platform>
</ProjectConfiguration>
<ProjectConfiguration Include="Release|x64">
<Configuration>Release</Configuration>
<Platform>x64</Platform>
</ProjectConfiguration>
</ItemGroup>
<ItemGroup>
<ClCompile Include="..\..\programs\ssl\mini_client.c" />
</ItemGroup>
<ItemGroup>
<ProjectReference Include="mbedTLS.vcxproj">

<Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
</ProjectReference>
</ItemGroup>
<PropertyGroup Label="Globals">
<ProjectGuid>{C4FE29EA-266D-5295-4840-976B9B5B3843}</ProjectGuid>
<Keyword>Win32Proj</Keyword>
<RootNamespace>mini_client</RootNamespace>
</PropertyGroup>
<Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
<PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
<ConfigurationType>Application</ConfigurationType>

```
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
/>
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <LinkIncremental>true</LinkIncremental>
```

```
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
     <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
 <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
```

```
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
   </Link>
   <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
   </ProjectReference>
  </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
   <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
   </Link>
  </ItemDefinitionGroup>
   <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
   <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
   <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
   </Link>
  </ItemDefinitionGroup>
```

```
 <Import
 Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
0_38IoSIKs0m
*H=42Qu0pSrgvtT$,hTxX'
-----BEGIN CERTIFICATE REQUEST-----
MIIBFzCBvwIBADA0MQswCQYDVQQGEwJOTDERMA8GA1UEChMIUG9sYXJTU0wxEjAQ
BgNVBAMTCWxvY2FsaG9zdDBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABDfMVtl2
CR5acj7HWS3/IG7ufPkGkXTQrRS192giWWKSTuUA2CMR/+ov0jRdXRa9iojCa3cN
Vc2KKg76Aci07f+gKTAnBgkqhkiG9w0BCQ4xGjAYMAkGA1UdEwQCMAAwCwYDVR0P
BAQDAgXgMAoGCCqGSM49BAMDA0cAMEQCIDnO+PIPZJGqiky9unvq13uXxahw1bpk
Zb5NRV0c06Q5AiAo5B49tp3kDN/n0BDNt1BBGLUfhcU+Qn2SQenCyfuGLg==
-----END CERTIFICATE REQUEST-----
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
   <Configuration>Release</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\pkey\rsa_genkey.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">

   <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid>{F472475C-F677-0E7F-F127-45BF5B64F622}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
```

```
  <RootNamespace>rsa_genkey</RootNamespace>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
 />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
```

```
    <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
  </PropertyGroup>
  <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
   <LinkIncremental>true</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
  </PropertyGroup>
  <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
   <LinkIncremental>false</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
  </PropertyGroup>
  <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
   <LinkIncremental>false</LinkIncremental>
   <IntDir>$(Configuration)\$(TargetName)\</IntDir>
  </PropertyGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
     <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
   </Link>
   <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
   </ProjectReference>
  </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
   <ClCompile>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <WarningLevel>Level3</WarningLevel>
     <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
   </ClCompile>
   <Link>
    <SubSystem>Console</SubSystem>
```

```
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
```

```
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
 <Import
 Project="$(VCTargetsPath)\Microsoft.Cpp.targets" />
 <ImportGroup Label="ExtensionTargets">
 </ImportGroup>
</Project>
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-192-CBC,72F869F41B989D71730B2983448251B8

R6ST6H9oUyFWBavUO++azbn9ga87lgeuqNMVVScOcXjguqQZdnuZq9AzwQQETEv+
ZbVPL9w2isuXKoavaPxYyCXbZ+l6JRfWiXi6CmnfNhx4MgYpbH9BEqGbIVxA3fvu
zFutqi+Ru6QeERshDNke6HfFjJ91WkBjNjrXcfDmt0uRGqFSWd5DSEniyaPmxCYs
mpRwr9XESFiBkCHL+/iSkW0EZBjwHW0//RNsZKtuqVJGW/dZhDxerOGRl0a1oWkb
IvfED7afrXMlpHokMwtUduk2TBE1AoczZ6Dv7RZGipaBR4yb9kYgIkiqFk53lg5h
7b3WQt6TYECI7X3Q2rDgPQtUChVud0uUQYmQ5328HRE8zhlWxHGmTQMWVBW6X+FM
ikFLRUeYBeq0UJu20DmvklZV6iDxsULLu+Rb0b8NkT+V2feSXbrP976oCSUznvT6
3e2EOH+KAqMy5JZhTsjM7HtkleMwYQ9v+Wnbnn1OsB9drYWUJuhQeXt6v8dkm/eD
9m6dZzivc/h1UThIuuZPo+6S7FoluIlt5uv2UcnYYdYOgKSd1Vm0wztGaJn3CSGw
JEbebucr+5ptOHxflV5Txgnfj63sJyVd/wy0T8sMRO2znk5uVLWxf855fNXev9M3
gA3+MXC2eGaR9DYOxfakFRwL+Z30RlIktaqDK76BZRD4sWB6dIVw5JdCXpNMCuDH
dxlTKcP59uPAEB2VyhDvm5CN3T+bM2K6WDZFO95hKKfEk5ea/UB7DA2ucfovdayE
Hd46EUKC4/cdUFiSycgD01ztdda7hU7hFvOkHTK7O3G1yvEwH0+jxKNsudNfbbxc
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTAwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATZwR+WK6NB
F/7riFdN63c8hjYddZRR4lrzVNPwiBQxnnxwpPyrD9A6aPPmLc6SqGOJW4ZGVCco
IBze9RJVeiB9o4GJMIGGMB0GA1UdDgQWBBSOSt6ePyMRT6PGMaIi7FqNX9MKtDBX
BgNVHSMEUDBOgBQtxZSLJAkEz+2RKMQexM6EtsfgcqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA5ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgN//NqM0FrkrMjmxoeCY9DgxkH2R6sQ4d
NgtwCZAIqEICIBs4vupaVcuvni9tltbP26wi7c0FR+blZuo5DPIA3SVe
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDkwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTAwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAR6jlGKbJd5
hiDxN789gkOcwpyHI9wRwCrADAOwOkMePBPRlwGdm7mw7Z/EAmu26zRm/hcyrs4M
qk2LabDjPI9Xo4GJMIGGMB0GA1UdDgQWBBQtxZSLJAkEz+2RKMQexM6EtsfgcjBX
BgNVHSMEUDBOgBT6gyXHzPIPYc1Vr1aGiLLeMh4HpqEzpDEwLzELMAkGA1UEBhMC
```

VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA4ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgP7S8vFstfUBdNe6ym5GYG5Q+aBVEKqRs
fVW7HNUktSYCIQDo6Jua6o/DJbrpq4qYWq5gv4yGyzPTN+3IaKrEICdaaw==
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDgwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDkwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAR7ZB16+t6E
sfahGyKUGJW5mezkzjdaYvc4lbJaKNRwFRfc3F/fmNOSsUFSg/F0N+vUE+doKiPC
8wRwLzvm4s+5o4GJMIGGMB0GA1UdDgQWBBT6gyXHzPIPYc1Vr1aGiLLeMh4HpjBX
BgNVHSMEUDBOgBS40mLt93U8Sh8ZGiDVAhRSiBPcXqEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA3ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgO4el1ZPhlIli/qNR2SIEiuvs5Mmy868i
N2Rv5X/VxIECIA/8rUALQxW38XSdBVX3e/jzu7ju47n1YwEqD9K9WdVv
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDcwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDgwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAARpQeQ/YGQj
nl7Szo6WStJ1u7xunTL5jBkXH8aAVSm0qiX4AD/7YPxa5EnGzZdLTn25vQVnfQAG
pMx8P1lYiGYCo4GJMIGGMB0GA1UdDgQWBBS40mLt93U8Sh8ZGiDVAhRSiBPcXjBX
BgNVHSMEUDBOgBREq5J3toJPxZ3O+ssJ5vkkU0RJE6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA2ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhANwGf+F4a+kmXWz8UjSpRkaToTV6EFWw
/Tjzj0tQhDoAAiEA19RxeWOVBBpM6LOHg6v5Lf54YN1snkLf+sEXyZCuWQQ=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDYwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDcwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASNOj4d4MEA
7p/3miijqG4ToE4opKPAm+3BTIGrJTYT14++TSiUICl0ASXj+xeUcLMIaXTN042s
LsHxpShzQaL0o4GJMIGGMB0GA1UdDgQWBBREq5J3toJPxZ3O+ssJ5vkkU0RJEzBX
BgNVHSMEUDBOgBSjovYaC/m6Li9Tp0V9iZRs9267Q6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA1ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAKGcf+c442c/XiwubbaiQvsoZ7EoVxuM
oKmia0gPyBNkAiEA83asjJ5FDXQuLyZpczviXrbmqgCPOfYadtvkc0cxMis=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDUwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDYwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASA9qWoAUHr

nn+3kxyNrjPJk82WDLimW21RN51uxpobadv8YgGEDRdP+Ok+uRqQSUsA6ZXfF3iG
r2GjfQ3wMDH8o4GJMIGGMB0GA1UdDgQWBBSjovYaC/m6Li9Tp0V9iZRs9267QzBX
BgNVHSMEUDBOgBTXh06MAV9S4l4lG1TKOrKRBh4qn6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTA0ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgcjZNFWJtlDmoPZbAxqsGczRYK0lfPgu6
g1H7pp0ce+wCIDj9BRZM2OB9EF0e+MDKGjyZGfvfrL6Ir47x/KrM6H8T
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDQwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDUwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQEdT0OFf5G
UcrgX2XllCyJzP94NZ464GsgB6psNLsDeL+j7AU+oJy7VLvW/lHh3ODgl08Z9bhq
LFBmNjnHbm8Qo4GJMIGGMB0GA1UdDgQWBBTXh06MAV9S4l4lG1TKOrKRBh4qnzBX
BgNVHSMEUDBOgBQox4F1NsZunlsduoGvzIgRSYfB36EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAzggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAIW++zqDZlLLUk/emePohdNOp5JO3wS9
XvkBJ6Wua7GBAiAdx+EKmdjVrwnzrQltTgnmSfGMXhKNYifK3uD83W3pcQ==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDMwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDQwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQUXDgcUVNT
9hovbZE5HL6rjOb7C55wEuWKThV/CcZ4rWrXx7VXHYdD/R3aDA7JSvYpm2sTok4i
sblDzhZM/GDNo4GJMIGGMB0GA1UdDgQWBBQox4F1NsZunlsduoGvzIgRSYfB3zBX
BgNVHSMEUDBOgBQApzZdtBdD3dLxouQpr/aDiVttd6EzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAyggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgAkiNhqFAZXSUWEDK91OZvQGdeZOtd6mC
+Wv3fGk3t28CIEKOwidkUTUaiPdZ4efmAr+CEeGzdq27ob2S+nqqHqgV
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB2DCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDIwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDMwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQRDXDNIi1p
ereudhqwa2LslXgsxnB63Hu5y5lg+1WPruIYPzD/Ho0APveVdzFLVji19+bE4+tF
PYL1SpsN1WfWo4GJMIGGMB0GA1UdDgQWBBQApzZdtBdD3dLxouQpr/aDiVttdzBX
BgNVHSMEUDBOgBT5RCgQ0AlZTQbfFB2+6+w0XRvydaEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAxggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSQAwRgIhAOnd+7bAofkHVa4KFNjv3TCegw1lrhuM
8Of8wgvrTEGoAiEAsS8iKMpSfXH4D0egg4gLamE6akde965rDtySU+ve9lg=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G

A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDEwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDIwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQWHpv1i6lf
wvNPOP5ka6S0n55EvzoaYK6pbTXP6yMOW/4XZSPKx5Zoq4FMe0cKzGIIFL1rzj1V
2czYB+qvLhyio4GJMIGGMB0GA1UdDgQWBBT5RCgQ0AlZTQbfFB2+6+w0XRvydTBX
BgNVHSMEUDBOgBSh3uHkX5nj86yFEFwjscSWM40P+qEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIhAI7unGW/gr9tOc3i+dF5N815srgh+FrX
oj9Et74EcSpTAiBubv+vOH0DE0gmYI11HeAIgutWqqMIC72dZlwTF/Vi3g==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB3jCCAYWgAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMDAwHhcNMTcwNjIyMTE1MDMyWhcN
MjcwNjIzMTE1MDMyWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMDEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQznn9zHHwL
GO8VR4W9V7vMlxCdoojzEOiX5Y6JtPtFOz866ueHY6zoN0/mJ6DnqnSXilJIUUeW
6eGfqmka7nxko4GRMIGOMB0GA1UdDgQWBBSh3uHkX5nj86yFEFwjscSWM40P+jBf
BgNVHSMEWDBWgBQlFYvU5WboI4fcdPoiQs8/fPHZraEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTAwggkA/KCWhcqToHAw
DAYDVR0TBAUwAwEB/zAKBggqhkjOPQQDAgNHADBEAiBasbuinP+pJTU4oDCVD8zQ
1rJBDSOKIEyWu84/D6Hj6wIgVMPUoO01bPhzllAa/gW8Xk/daey09SBgN3AT9pWU
TDA=
-----END
CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIBpTCCAUugAwIBAgIJAPygloXKk6BwMAoGCCqGSM49BAMCMC8xCzAJBgNVBAYT
AlVLMREwDwYDVQQKDAhtYmVkIFRMUzENMAsGA1UEAwwEQ0EwMDAeFw0xNzA2MjIx
MTUwMzJaFw0yNzA2MjMxMTUwMzJaMC8xCzAJBgNVBAYTAlVLMREwDwYDVQQKDAht
YmVkIFRMUzENMAsGA1UEAwwEQ0EwMDBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IA
BFW41/qAwAPpy+Txdc7PKmzZsq9CPiujKU4vpF1ekXnGx2HP420QobwBVVWhkzRm
LwdboH2j65dcCKjQ7mv/dxKjUDBOMB0GA1UdDgQWBBQlFYvU5WboI4fcdPoiQs8/
fPHZrTAfBgNVHSMEGDAWgBQlFYvU5WboI4fcdPoiQs8/fPHZrTAMBgNVHRMEBTAD
AQH/MAoGCCqGSM49BAMCA0gAMEUCIQC7iRcVzwMyfVK5imirJ7MqJQ04euH4CLOt
IZ+SNfaERAIgSU0MWFDosVEIpg8YMqIHeF7Mg4ZyH6+fGazJgVLttUY=
-----END
CERTIFICATE-----
Purpose:
- To test and prove that a new commit in the mbed TLS repository builds
and integrates with mbed-os properly.
AND
- To test and prove that the current development head of mbed TLS builds
and integrates with the current mbed-os master branch.
#
The script fetches all the prerequisites and builds the mbed TLS 'tls-client'
example. This script is triggered by every commit and once each night and the
exact behaviour depends on how it was triggered:
- If it is a nightly build then it builds the mbed TLS development head with
mbed-os master.

```
# - If it was triggered by the commit, then it builds the example with mbed TLS
#   at that commit and mbed-os at the commit pointed by mbed-os.lib in the
#   example repository.

test:
  override:
    - cd ../mbed-os-example-tls/tls-client/ && mbed compile -m K64F -t GCC_ARM -c

dependencies:
  pre:
    # Install gcc-arm
    - cd .. && wget "https://launchpad.net/gcc-arm-embedded/4.9/4.9-2015-q3-update/+download/gcc-arm-none-
eabi-4_9-2015q3-20150921-linux.tar.bz2"
     - cd .. && tar -xvjf gcc-arm-none-eabi-4_9-2015q3-20150921-linux.tar.bz2
    - ln -s ../gcc-arm-none-eabi-4_9-2015q3/bin/* ../bin/
    # Install mbed-cli
    - cd ../ && git clone https://github.com/ARMmbed/mbed-cli.git
    - cd ../mbed-cli && sudo -H pip install -e .
    # Get the sample application
    - cd ../ && git clone git@github.com:ARMmbed/mbed-os-example-tls.git
    # Get mbed-os
    - cd ../mbed-os-example-tls/tls-client && mbed deploy
    # Update mbed-os to master only if it is a nightly build
    - >
      if [ -n "${RUN_NIGHTLY_BUILD}" ]; then
        cd ../mbed-os-example-tls/tls-client/mbed-os/ && mbed update master;
      fi
    # Import mbedtls current revision
    - ln -s ../../../../../../mbedtls/ ../mbed-os-example-tls/tls-client/mbed-
os/features/mbedtls/importer/TARGET_IGNORE/mbedtls
    - cd ../mbed-os-example-tls/tls-client/mbed-os/features/mbedtls/importer/
 && make
  override:
    # Install the missing python packages
    - cd ../mbed-os-example-tls/tls-client/mbed-os/ && sudo -H pip install -r requirements.txt
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-CBC,AA94892A169FA426

gSkFuUENNke5MvkWHc11/w1NQWBxaIxGT+d5oRcqs44D3tltVOwtdnYexoD9uSIL
wMFFRLL6I5ii1Naa38nPOMaa7kLU2J3jY8SeIH1rQ43X6tlpv9WFGqDn/m6X7oKo
RMMfGdicPZg=
-----END EC PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIB1jCCAX2gAwIBAgIBATAKBggqhkjOPQQDAjAvMQswCQYDVQQGEwJVSzERMA8G
A1UECgwIbWJlZCBUTFMxDTALBgNVBAMMBENBMTgwHhcNMTcwNjIyMTE1MDMzWhcN
MjcwNjIzMTE1MDMzWjAvMQswCQYDVQQGEwJVSzERMA8GA1UECgwIbWJlZCBUTFMx
DTALBgNVBAMMBENBMTkwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQJyRCHND78
```

```
KxZHoHHdOTjPuD6HjHPnEKX8apblUpETDJuLW7YR3V8Q0dTac+JHiR6e2l4DlDbf
5bTiyFoAzw9yo4GJMIGGMB0GA1UdDgQWBBRQMc94kTqW+zQO3lo2WMI/81k3czBX
BgNVHSMEUDBOgBSDbIpYntlhJ0GgIsyd75XRhlC18qEzpDEwLzELMAkGA1UEBhMC
VUsxETAPBgNVBAoMCG1iZWQgVExTMQ0wCwYDVQQDDARDQTE3ggEBMAwGA1UdEwQF
MAMBAf8wCgYIKoZIzj0EAwIDRwAwRAIgIzGOZqJRmvygzvLm8zxZFyoNpcT7e26H
nZd5xFIzEakCIHGYcUXzt+owSVlLmrlW8gQcB81ErQbxuBTAsvpaaKSS
-----END CERTIFICATE-----
<?xml version="1.0" encoding="utf-8"?>
<Project DefaultTargets="Build" ToolsVersion="4.0"
xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <ItemGroup Label="ProjectConfigurations">
  <ProjectConfiguration Include="Debug|Win32">
   <Configuration>Debug</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Debug|x64">
   <Configuration>Debug</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|Win32">
   <Configuration>Release</Configuration>
   <Platform>Win32</Platform>
  </ProjectConfiguration>
  <ProjectConfiguration Include="Release|x64">
   <Configuration>Release</Configuration>
   <Platform>x64</Platform>
  </ProjectConfiguration>
 </ItemGroup>
 <ItemGroup>
  <ClCompile Include="..\..\programs\pkey\gen_key.c" />
 </ItemGroup>
 <ItemGroup>
  <ProjectReference Include="mbedTLS.vcxproj">

 <Project>{46cf2d25-6a36-4189-b59c-e4815388e554}</Project>
  </ProjectReference>
 </ItemGroup>
 <PropertyGroup Label="Globals">
  <ProjectGuid>{BF782A50-E9AE-00CC-C28A-C9DA8AAB4D52}</ProjectGuid>
  <Keyword>Win32Proj</Keyword>
  <RootNamespace>gen_key</RootNamespace>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.Default.props" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
```

```
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>true</UseDebugLibraries>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'" Label="Configuration">
   <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="Configuration">
  <ConfigurationType>Application</ConfigurationType>
  <UseDebugLibraries>false</UseDebugLibraries>
  <WholeProgramOptimization>true</WholeProgramOptimization>
  <CharacterSet>Unicode</CharacterSet>
  <PlatformToolset>Windows7.1SDK</PlatformToolset>
 </PropertyGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.props" />
 <ImportGroup Label="ExtensionSettings">
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform"
 />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Label="PropertySheets" Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <ImportGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'" Label="PropertySheets">
  <Import Project="$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props"
Condition="exists('$(UserRootDir)\Microsoft.Cpp.$(Platform).user.props')" Label="LocalAppDataPlatform" />
 </ImportGroup>
 <PropertyGroup Label="UserMacros" />
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
   <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <LinkIncremental>true</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
```

```
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <PropertyGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <LinkIncremental>false</LinkIncremental>
  <IntDir>$(Configuration)\$(TargetName)\</IntDir>
 </PropertyGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|Win32'">
  <ClCompile>
   <PrecompiledHeader>
   </PrecompiledHeader>
   <WarningLevel>Level3</WarningLevel>
   <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
    <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
   <SubSystem>Console</SubSystem>
   <GenerateDebugInformation>true</GenerateDebugInformation>
   <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
   <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  <ClCompile>
   <PrecompiledHeader>
   </PrecompiledHeader>
   <WarningLevel>Level3</WarningLevel>
    <Optimization>Disabled</Optimization>
<PreprocessorDefinitions>WIN32;_DEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
 <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
   <SubSystem>Console</SubSystem>
   <GenerateDebugInformation>true</GenerateDebugInformation>
   <ShowProgress>NotSet</ShowProgress>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole32.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependencies>
    <AdditionalLibraryDirectories>Debug</AdditionalLibraryDirectories>
  </Link>
  <ProjectReference>
```

```
    <LinkLibraryDependencies>false</LinkLibraryDependencies>
  </ProjectReference>
 </ItemDefinitionGroup>
 <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|Win32'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
     <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN32;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
<AdditionalDependencies>kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;advapi32.lib;shell32.lib;ole3
2.lib;oleaut32.lib;uuid.lib;odbc32.lib;odbccp32.lib;%(AdditionalDependencies);mbedTLS.lib</AdditionalDependen
cies>
  </Link>
 </ItemDefinitionGroup>
  <ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Release|x64'">
  <ClCompile>
    <WarningLevel>Level3</WarningLevel>
    <PrecompiledHeader>
    </PrecompiledHeader>
    <Optimization>MaxSpeed</Optimization>
    <FunctionLevelLinking>true</FunctionLevelLinking>
    <IntrinsicFunctions>true</IntrinsicFunctions>
<PreprocessorDefinitions>WIN64;NDEBUG;_CONSOLE;%(PreprocessorDefinitions)</PreprocessorDefinitions>
  <AdditionalIncludeDirectories>../../include</AdditionalIncludeDirectories>
  </ClCompile>
  <Link>
    <SubSystem>Console</SubSystem>
    <GenerateDebugInformation>true</GenerateDebugInformation>
    <EnableCOMDATFolding>true</EnableCOMDATFolding>
    <OptimizeReferences>true</OptimizeReferences>
    <AdditionalLibraryDirectories>Release</AdditionalLibraryDirectories>
    <AdditionalDependencies>%(AdditionalDependencies);</AdditionalDependencies>
  </Link>
 </ItemDefinitionGroup>
 <Import Project="$(VCTargetsPath)\Microsoft.Cpp.targets"
 />
 <ImportGroup Label="ExtensionTargets">
```

</ImportGroup>
</Project>
-----BEGIN CERTIFICATE-----
MIICHjCCAaWgAwIBAgIBHjAKBggqhkjOPQQDAjA+MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EwHhcN
MDQwMzEwMTIwOTMwWhcNMTQwMzA4MTIwOTMwWjA0MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxEjAQBgNVBAMTCWxvY2FsaG9zdDBZMBMGByqGSM49AgEG
CCqGSM49AwEHA0IABDfMVtl2CR5acj7HWS3/IG7ufPkGkXTQrRS192giWWKSTuUA
2CMR/+ov0jRdXRa9iojCa3cNVc2KKg76Aci07f+jgZ0wgZowCQYDVR0TBAIwADAd
BgNVHQ4EFgQUUGGlj9QH2deCAQzlZX+MY0anE74wbgYDVR0jBGcwZYAUnW0gJEkB
PyvLeLUZvH4kydv7NnyhQqRAMD4xCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQb2xh
clNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBFQyBDQYIJAMFD4n5iQ8zoMAoG
CCqGSM49BAMCA2cAMGQCMCDxvDmhlrEk0r4hqCwvQDxWEoXPbbD1gglfLT3BsGpu
XHUQ1W2HwB3o/7N5I13BBgIwcmG17zyNIOkYiyExYtPCZCpbofEMpRY5qWG0K6YL
fN08jSzyFt6kbO4ak0D6tC5Q
-----END CERTIFICATE-----
Camellia-GCM test vect draft-kato-ipsec-camellia-gcm #1 (128-en)
depends_on:MBEDTLS_CAMELLIA_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"00000000000000000000000000000000":"":"00000000000000000000000000":"":"":128:"f5574acc3148dfcb9015200631024df9":0

Camellia-GCM test vect draft-kato-ipsec-camellia-gcm #2 (128-en)
depends_on:MBEDTLS_CAMELLIA_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"00000000000000000000000000000000":"000000000000000000000000":"00000000000000000000000000":"":"defe3e0b5c54c94b4f2a0f5a46f6210d":128:"f672b94d192266c7c8c8dbb427cc989a":0

Camellia-GCM test vect draft-kato-ipsec-camellia-gcm #3 (128-en)
depends_on:MBEDTLS_CAMELLIA_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308":"d9313225f88406e5a55909c5aff5269a86a7a9531534f7da2e4c303d8a318a721c3c0c95956809532fcf0e2449a6b525b16aedf5aa0de657ba637b391aafd255":"cafebabefacedbaddecaf888":"":"d0d94a13b632f337a0cc9955b94fa020c815f903aab12f1efaf2fe9d90f729a6cccbfa986ef2ff2c33de418d9a2529091cf18fe652c1cfde13f8260614bab815":128:"86e318012dd8329dc9dae6a170f61b24":0

Camellia-GCM
test vect draft-kato-ipsec-camellia-gcm #4 (128-en)
depends_on:MBEDTLS_CAMELLIA_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308":"d9313225f88406e5a55909c5aff5269a86a7a9531534f7da2e4c303d8a318a721c3c0c95956809532fcf0e2449a6b525b16aedf5aa0de657ba637b39":"cafebabefacedbaddecaf888":"feedfacedeadbeeffeedfacedeadbeefabaddad2":"d0d94a13b632f337a0cc9955b94fa020c815f903aab12f1efaf2fe9d90f729a6cccbfa986ef2ff2c33de418d9a2529091cf18fe652c1cfde13f82606":128:"9f458869431576ea6a095456ec6b8101":0

Camellia-GCM test vect draft-kato-ipsec-camellia-gcm #5 (128-en)
depends_on:MBEDTLS_CAMELLIA_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308":"d9313225f88406e5a55909c5aff5269a86a7a9531534f7da2e4c303d8a318a721c3c0c95956809532fcf0e2449a6b525b16aedf5aa0

de657ba637b39":"cafebabefacedbad":"feedfacedeadbeeffeedfacedeadbeefabaddad2":"28fd7434d5cd424a5353818fc
21a982460d20cf632eb1e6c4fbfca17d5abcf6a52111086162fe9570e7774c7a912aca3dfa10067ddaad40688645bdd":1
28:"e86f8f2e730c49d536f00fb5225d28b1":0

Camellia-GCM
test vect draft-kato-ipsec-camellia-gcm #6 (128-en)
depends_on:MBEDTLS_CAMELLIA_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308":"d9313225f
88406e5a55909c5aff5269a86a7a9531534f7da2e4c303d8a318a721c3c0c95956809532fcf0e2449a6b525b16aedf5aa0
de657ba637b39":"9313225df88406e555909c5aff5269aa6a7a9538534f7da1e4c303d2a318a728c3c0c95156809539fc
f0e2429a6b525416aedbf5a0de6a57a637b39b":"feedfacedeadbeeffeedfacedeadbeefabaddad2":"2e582b8417c93f2ff4
f6f7ee3c361e4496e710ee12433baa964987d02f42953e402e6f4af407fe08cd2f35123696014c34db19128df4056faebc
d647":128:"ceae5569b2af8641572622731aed3e53":0

Camellia-GCM test vect draft-kato-ipsec-camellia-gcm #7 (192-en)
depends_on:MBEDTLS_CAMELLIA_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"000000000000000000000000000000000000000000000000
000000":"":"000000000000000000000000":"":"":128:"ba9ae89fddce4b51131e17c4d65ce587":0

Camellia-GCM
test vect draft-kato-ipsec-camellia-gcm #8 (192-en)
depends_on:MBEDTLS_CAMELLIA_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"000000000000000000000000000000000000000000000000
000000":"000000000000000000000000000000000":"000000000000000000000000":"":"8f9c0aa2549714c88bb2665
e8af86d41":128:"783cff5c5aca7197320658a74279ab37":0

Camellia-GCM test vect draft-kato-ipsec-camellia-gcm #9 (192-en)
depends_on:MBEDTLS_CAMELLIA_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308feffe99286657
31c":"d9313225f88406e5a55909c5aff5269a86a7a9531534f7da2e4c303d8a318a721c3c0c95956809532fcf0e2449a6
b525b16aedf5aa0de657ba637b391aafd255":"cafebabefacedbaddecaf888":"":"0f009e88410d84ad93c90d55efbe20ff
a855492f4dfd0fb485c4f02f536feffbb4d967729e5c67f1de0750255cc500716ba483eb3b0a2bf607af28f6a60bb2e9":1
28:"8d645a0b0e48d3c3b60a014157cb49b4":0

Camellia-GCM test vect draft-kato-ipsec-camellia-gcm #10 (192-en)
depends_on:MBEDTLS_CAMELLIA_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308feffe99286657
31c":"d9313225f88406e5a55909c5aff5269a86a7a9531534f7da2e4c303d8a318a721c3c0c95956809532fcf0e2449a6
b525b16aedf5aa0de657ba637b39":"cafebabefacedbaddecaf888":"feedfacedeadbeeffeedfacedeadbeefabaddad2":"0f0
09e88410d84ad93c90d55efbe20ffa855492f4dfd0fb485c4f02f536feffbb4d967729e5c67f1de0750255cc500716ba483
eb3b0a2bf607af28f6":128:"01b15bb5ab6fac0c422014e91eacbf2b":0

Camellia-GCM
test vect draft-kato-ipsec-camellia-gcm #11 (192-en)
depends_on:MBEDTLS_CAMELLIA_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308feffe99286657
31c":"d9313225f88406e5a55909c5aff5269a86a7a9531534f7da2e4c303d8a318a721c3c0c95956809532fcf0e2449a6
b525b16aedf5aa0de657ba637b39":"cafebabefacedbad":"feedfacedeadbeeffeedfacedeadbeefabaddad2":"678b3dcb27

0faa206dc5f6fbb5014996e86d6f3e35cdcdfeb03b37b9b06ff4ff2682248823bd3c84124dc76af7bde3dd440c228b5efb
c795dd80dfb6":128:"f876143d933214a5035ff0bb96ff650b":0

Camellia-GCM
test vect draft-kato-ipsec-camellia-gcm #12 (192-en)
depends_on:MBEDTLS_CAMELLIA_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308feffe99286657
31c":"d9313225f88406e5a55909c5aff5269a86a7a9531534f7da2e4c303d8a318a721c3c0c95956809532fcf0e2449a6
b525b16aedf5aa0de657ba637b39":"9313225df88406e555909c5aff5269aa6a7a9538534f7da1e4c303d2a318a728c3c
0c95156809539fcf0e2429a6b525416aedbf5a0de6a57a637b39b":"feedfacedeadbeeffeedfacedeadbeefabaddad2":"97
33ea567c3bad2259ccd63ef7012f5de709e50b1fdc31f1a16db02ede1b66f11dcc4d953f2d4d4671587b65882afbf9545f
db6deab22413d091b703":128:"4b72e520b2521e63d240ed5c903216fa":0

Camellia-GCM test vect draft-kato-ipsec-camellia-gcm #13 (256-en)
depends_on:MBEDTLS_CAMELLIA_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"000000000000000000000000000000000000000000000000
0000000000000000000000":"":"000000000000000000000000":"":"":128:"9cdb269b5d293bc5db9c55b057d9b591":
0

Camellia-GCM test vect draft-kato-ipsec-camellia-gcm #14 (256-en)
depends_on:MBEDTLS_CAMELLIA_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"000000000000000000000000000000000000000000000000
0000000000000000000000":"00000000000000000000000000000000":"000000000000000000000000":"":"3d4b2c
de666761ba5dfb305178e667fb":128:"284b63bb143c40ce100fb4dea6bb617b":0

Camellia-GCM
test vect draft-kato-ipsec-camellia-gcm #15 (256-en)
depends_on:MBEDTLS_CAMELLIA_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308feffe99286657
31c6d6a8f9467308308":"d9313225f88406e5a55909c5aff5269a86a7a9531534f7da2e4c303d8a318a721c3c0c95956
809532fcf0e2449a6b525b16aedf5aa0de657ba637b391aafd255":"cafebabefacedbaddecaf888":"":"ad142c11579dd95
e41f3c1f324dabc255864d920f1b65759d8f560d4948d447758dfdcf77aa9f62581c7ff572a037f810cb1a9c4b3ca6ed63
8179b776549e092":128:"c912686270a2b9966415fca3be75c468":0

Camellia-GCM test vect draft-kato-ipsec-camellia-gcm #16 (256-en)
depends_on:MBEDTLS_CAMELLIA_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308feffe99286657
31c6d6a8f9467308308":"d9313225f88406e5a55909c5aff5269a86a7a9531534f7da2e4c303d8a318a721c3c0c95956
809532fcf0e2449a6b525b16aedf5aa0de657ba637b39":"cafebabefacedbaddecaf888":"feedfacedeadbeeffeedfacedead
beefabaddad2":"ad142c11579dd95e41f3c1f324dabc255864d920f1b65759d8f560d4948d447758dfdcf77aa9f62581c
7ff572a037f810cb1a9c4b3ca6ed638179b77":128:"4e4b178d8fe26fdc95e2e7246dd94bec":0

Camellia-GCM
test vect draft-kato-ipsec-camellia-gcm #17 (256-en)
depends_on:MBEDTLS_CAMELLIA_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308feffe99286657
31c6d6a8f9467308308":"d9313225f88406e5a55909c5aff5269a86a7a9531534f7da2e4c303d8a318a721c3c0c95956
809532fcf0e2449a6b525b16aedf5aa0de657ba637b39":"cafebabefacedbad":"feedfacedeadbeeffeedfacedeadbeefabad

dad2":"6ca95fbb7d16577a9ef2fded94dc85b5d40c629f6bef2c649888e3cbb0ededc7810c04b12c2983bbbbc482e16e4
5c9215ae12c15c55f2f4809d06652":128:"e6472b8ebd331bfcc7c0fa63ce094461":0

Camellia-GCM test vect draft-kato-ipsec-camellia-gcm
#18 (256-en)
depends_on:MBEDTLS_CAMELLIA_C
gcm_encrypt_and_tag:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308feffe99286657
31c6d6a8f9467308308":"d9313225f88406e5a55909c5aff5269a86a7a9531534f7da2e4c303d8a318a721c3c0c95956
809532fcf0e2449a6b525b16aedf5aa0de657ba637b39":"9313225df88406e555909c5aff5269aa6a7a9538534f7da1e4
c303d2a318a728c3c0c95156809539fcf0e2429a6b525416aedbf5a0de6a57a637b39b":"feedfacedeadbeeffeedfacedea
dbeefabaddad2":"e0cddd7564d09c4dc522dd65949262bbf9dcdb07421cf67f3032becb7253c284a16e5bf0f556a30804
3f53fab9eebb526be7f7ad33d697ac77c67862":128:"5791883f822013f8bd136fc36fb9946b":0

Camellia-GCM test vect draft-kato-ipsec-camellia-gcm #1 (128-de)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"00000000000000000000000000000000":"":"000
00000000000000000000":"":128:"f5574acc3148dfcb9015200631024df9":"":0

Camellia-GCM test vect draft-kato-ipsec-camellia-gcm #2 (128-de)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"00000000000000000000000000000000":"defe3e
0b5c54c94b4f2a0f5a46f6210d":"000000000000000000000000":"":128:"f672b94d192266c7c8c8dbb427cc989a":"0
0000000000000000000000000000000":0

Camellia-GCM
test vect draft-kato-ipsec-camellia-gcm #3 (128-de)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308":"d0d94a1
3b632f337a0cc9955b94fa020c815f903aab12f1efaf2fe9d90f729a6cccbfa986ef2ff2c33de418d9a2529091cf18fe652c
1cfde13f8260614bab815":"cafebabefacedbaddecaf888":"":128:"86e318012dd8329dc9dae6a170f61b24":"d9313225
f88406e5a55909c5aff5269a86a7a9531534f7da2e4c303d8a318a721c3c0c95956809532fcf0e2449a6b525b16aedf5aa
0de657ba637b391aafd255":0

Camellia-GCM test vect draft-kato-ipsec-camellia-gcm #4 (128-de)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308":"d0d94a1
3b632f337a0cc9955b94fa020c815f903aab12f1efaf2fe9d90f729a6cccbfa986ef2ff2c33de418d9a2529091cf18fe652c
1cfde13f82606":"cafebabefacedbaddecaf888":"feedfacedeadbeeffeedfacedeadbeefabaddad2":128:"9f458869431576
ea6a095456ec6b8101":"d9313225f88406e5a55909c5aff5269a86a7a9531534f7da2e4c303d8a318a721c3c0c959568
09532fcf0e2449a6b525b16aedf5aa0de657ba637b39":0

Camellia-GCM
test vect draft-kato-ipsec-camellia-gcm #5 (128-de)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308":"28fd743
4d5cd424a5353818fc21a982460d20cf632eb1e6c4fbfca17d5abcf6a52111086162fe9570e7774c7a912aca3dfa10067d
daad40688645bdd":"cafebabefacedbad":"feedfacedeadbeeffeedfacedeadbeefabaddad2":128:"e86f8f2e730c49d536f0
0fb5225d28b1":"d9313225f88406e5a55909c5aff5269a86a7a9531534f7da2e4c303d8a318a721c3c0c95956809532fc

f0e2449a6b525b16aedf5aa0de657ba637b39":0

Camellia-GCM test vect draft-kato-ipsec-camellia-gcm #6 (128-de)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308":"2e582b8417c93f2ff4f6f7ee3c361e4496e710ee12433baa964987d02f42953e402e6f4af407fe08cd2f35123696014c34db19128df4056faebcd647":"9313225df88406e555909c5aff5269aa6a7a9538534f7da1e4c303d2a318a728c3c0c95156809539fcf0e2429a6b525416aedbf5a0de6a57a637b39b":"feedfacedeadbeeffeedfacedeadbeefabaddad2":128:"ceae5569b2af8641572622731aed3e53":"d9313225f88406e5a55909c5aff5269a86a7a9531534f7da2e4c303d8a318a721c3c0c95956809532fcf0e2449a6b525b16aedf5aa0de657ba637b39":0

Camellia-GCM
test vect draft-kato-ipsec-camellia-gcm #7 (192-de)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"000000000000000000000000000000000000000000000000":"":"000000000000000000000000":"":128:"ba9ae89fddce4b51131e17c4d65ce587":"":0

Camellia-GCM test vect draft-kato-ipsec-camellia-gcm #8 (192-de)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"000000000000000000000000000000000000000000000000":"8f9c0aa2549714c88bb2665e8af86d41":"000000000000000000000000":"":128:"783cff5c5aca7197320658a74279ab37":"00000000000000000000000000000000":0

Camellia-GCM
test vect draft-kato-ipsec-camellia-gcm #9 (192-de)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308feffe9928665731c":"0f009e88410d84ad93c90d55efbe20ffa855492f4dfd0fb485c4f02f536feffbb4d967729e5c67f1de0750255cc500716ba483eb3b0a2bf607af28f6a60bb2e9":"cafebabefacedbaddecaf888":"":128:"8d645a0b0e48d3c3b60a014157cb49b4":"d9313225f88406e5a55909c5aff5269a86a7a9531534f7da2e4c303d8a318a721c3c0c95956809532fcf0e2449a6b525b16aedf5aa0de657ba637b391aafd255":0

Camellia-GCM test vect draft-kato-ipsec-camellia-gcm #10 (192-de)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308feffe9928665731c":"0f009e88410d84ad93c90d55efbe20ffa855492f4dfd0fb485c4f02f536feffbb4d967729e5c67f1de0750255cc500716ba483eb3b0a2bf607af28f6":"cafebabefacedbaddecaf888":"feedfacedeadbeeffeedfacedeadbeefabaddad2":128:"01b15bb5ab6fac0c422014e91eacbf2b":"d9313225f88406e5a55909c5aff5269a86a7a9531534f7da2e4c303d8a318a721c3c0c95956809532fcf0e2449a6b525b16aedf5aa0de657ba637b39":0

Camellia-GCM
test vect draft-kato-ipsec-camellia-gcm #11 (192-de)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308feffe9928665731c":"678b3dcb270faa206dc5f6fbb5014996e86d6f3e35cdcdfeb03b37b9b06ff4ff2682248823bd3c84124dc76af7bde3dd440c228b5efbc795dd80dfb6":"cafebabefacedbad":"feedfacedeadbeeffeedfacedeadbeefabaddad2":128:"f876143d933214a5035ff0bb96ff650b":"d9313225f88406e5a55909c5aff5269a86a7a9531534f7da2e4c303d8a318a721c3c0c95956809532fcf0e2449a6b525b16aedf5aa0de657ba637b39":0

Camellia-GCM test vect draft-kato-ipsec-camellia-gcm #12 (192-de)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308feffe9928665731c":"9733ea567c3bad2259ccd63ef7012f5de709e50b1fdc31f1a16db02ede1b66f11dcc4d953f2d4d4671587b65882afbf9545fdb6deab22413d091b703":"9313225df88406e555909c5aff5269aa6a7a9538534f7da1e4c303d2a318a728c3c0c95156809539fcf0e2429a6b525416aedbf5a0de6a57a637b39b":"feedfacedeadbeeffeedfacedeadbeefabaddad2":128:"4b72e520b2521e63d240ed5c903216fa":"d9313225f88406e5a55909c5aff5269a86a7a9531534f7da2e4c303d8a318a721c3c0c95956809532fcf0e2449a6b525b16aedf5aa0de657ba637b39":0

Camellia-GCM
test vect draft-kato-ipsec-camellia-gcm #13 (256-de)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"000000000000000000000000000000000000000000000000000000000000000000000000":"":"000000000000000000000000":"":128:"9cdb269b5d293bc5db9c55b057d9b591":"":0

Camellia-GCM test vect draft-kato-ipsec-camellia-gcm #14 (256-de)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"000000000000000000000000000000000000000000000000000000000000000000000000":"3d4b2cde666761ba5dfb305178e667fb":"000000000000000000000000":"":128:"284b63bb143c40ce100fb4dea6bb617b":"00000000000000000000000000000000":0

Camellia-GCM test vect draft-kato-ipsec-camellia-gcm
#15 (256-de)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308feffe9928665731c6d6a8f9467308308":"ad142c11579dd95e41f3c1f324dabc255864d920f1b65759d8f560d4948d447758dfdcf77aa9f62581c7ff572a037f810cb1a9c4b3ca6ed638179b776549e092":"cafebabefacedbaddecaf888":"":128:"c912686270a2b9966415fca3be75c468":"d9313225f88406e5a55909c5aff5269a86a7a9531534f7da2e4c303d8a318a721c3c0c95956809532fcf0e2449a6b525b16aedf5aa0de657ba637b391aafd255":0

Camellia-GCM test vect draft-kato-ipsec-camellia-gcm #16 (256-de)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308feffe9928665731c6d6a8f9467308308":"ad142c11579dd95e41f3c1f324dabc255864d920f1b65759d8f560d4948d447758dfdcf77aa9f62581c7ff572a037f810cb1a9c4b3ca6ed638179b77":"cafebabefacedbaddecaf888":"feedfacedeadbeeffeedfacedeadbeefabaddad2":128:"4e4b178d8fe26fdc95e2e7246dd94bec":"d9313225f88406e5a55909c5aff5269a86a7a9531534f7da2e4c303d8a318a721c3c0c95956809532fcf0e2449a6b525b16aedf5aa0de657ba637b39":0

Camellia-GCM
test vect draft-kato-ipsec-camellia-gcm #17 (256-de)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308feffe9928665731c6d6a8f9467308308":"6ca95fbb7d16577a9ef2fded94dc85b5d40c629f6bef2c649888e3cbb0ededc7810c04b12c2983bbbbc482e16e45c9215ae12c15c55f2f4809d06652":"cafebabefacedbad":"feedfacedeadbeeffeedfacedeadbeefabaddad2":128:"e6472b8ebd331bfcc7c0fa63ce094461":"d9313225f88406e5a55909c5aff5269a86a7a9531534f7da2e4c303d8a318a721c3c0c95956809532fcf0e2449a6b525b16aedf5aa0de657ba637b39":0

Camellia-GCM test vect draft-kato-ipsec-camellia-gcm #18 (256-de)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308feffe9928665731c6d6a8f9467308308":"e0cddd7564d09c4dc522dd65949262bbf9dcdb07421cf67f3032becb7253c284a16e5bf0f556a308043f53fab9eebb526be7f7ad33d697ac77c67862":"9313225df88406e555909c5aff5269aa6a7a9538534f7da1e4c303d2a318a728c3c0c95156809539fcf0e2429a6b525416aedbf5a0de6a57a637b39b":"feedfacedeadbeeffeedfacedeadbeefabaddad2":128:"5791883f822013f8bd136fc36fb9946b":"d9313225f88406e5a55909c5aff5269a86a7a9531534f7da2e4c303d8a318a721c3c0c95956809532fcf0e2449a6b525b16aedf5aa0de657ba637b39":0

Camellia-GCM
test vect draft-kato-ipsec-camellia-gcm #1 (128-bad)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"00000000000000000000000000000000":"":"00000000000000000000000":"":128:"f5574acc3148dfcb9015200631024df8":"FAIL":0

Camellia-GCM test vect draft-kato-ipsec-camellia-gcm #2 (128-bad)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"00000000000000000000000000000000":"defe3e0b5c54c94b4f2a0f5a46f7210d":"000000000000000000000000":"":128:"f672b94d192266c7c8c8dbb427cc989a":"FAIL":0

Camellia-GCM test vect draft-kato-ipsec-camellia-gcm #3 (128-bad)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308":"d0d94a13b632f337a0cc9955b94fa020c815f903aab12f1efaf2fe9d90f729a6cccbfa986ef2ff2c33de418d9a2529091cf18fe652c1cfde13f8260614bab815":"cafebabefacedbaddecaf889":"":128:"86e318012dd8329dc9dae6a170f61b24":"FAIL":0

Camellia-GCM
test vect draft-kato-ipsec-camellia-gcm #4 (128-bad)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308":"d0d94a13b632f337a0cc9955b94fa020c815f903aab12f1efaf2fe9d90f729a6cccbfa986ef2ff2c33de418d9a2529091cf18fe652c1cfde13f82606":"cafebabefacedbaddecaf888":"feedfacedeadbeeffeedfacedeadbeefabaddad2":128:"9f458869431576ea6a095456ec6b8100":"FAIL":0

Camellia-GCM test vect draft-kato-ipsec-camellia-gcm #5 (128-bad)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308":"28fd7434d5cd424a5353818fc21a982460d20cf632eb1e6c4fbfca17d5abcf6a52111086162fe9570e7774c7a912aca3dfa10067ddaad40688645bdd":"cafebabefacedbad":"feedfadedeadbeeffeedfacedeadbeefabaddad2":128:"e86f8f2e730c49d536f00fb5225d28b1":"FAIL":0

Camellia-GCM
test vect draft-kato-ipsec-camellia-gcm #6 (128-bad)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308":"2e582b8417c83f2ff4f6f7ee3c361e4496e710ee12433baa964987d02f42953e402e6f4af407fe08cd2f35123696014c34db19128

df4056faebcd647":"9313225df88406e555909c5aff5269aa6a7a9538534f7da1e4c303d2a318a728c3c0c95156809539fcf0e2429a6b525416aedbf5a0de6a57a637b39b":"feedfacedeadbeeffeedfacedeadbeefabaddad2":128:"ceae5569b2af8641572622731aed3e53":"FAIL":0

Camellia-GCM test vect draft-kato-ipsec-camellia-gcm #7 (192-bad)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"00000000000000000000000000000000000000000000000000000000":"":"000000000000000000000000":"":128:"ba9ae89fddce4b51131e17c4d65ce586":"FAIL":0

Camellia-GCM test vect draft-kato-ipsec-camellia-gcm #8 (192-bad)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"00000000000000000000000000000000000000000000000000000000":"8f9c0aa2549714c88bb2665e8af86d42":"000000000000000000000000":"":128:"783cff5c5aca7197320658a74279ab37":"FAIL":0

Camellia-GCM
test vect draft-kato-ipsec-camellia-gcm #9 (192-bad)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"ffffe9928665731c6d6a8f9467308308feffe9928665731c":"0f009e88410d84ad93c90d55efbe20ffa855492f4dfd0fb485c4f02f536feffbb4d967729e5c67f1de0750255cc500716ba483eb3b0a2bf607af28f6a60bb2e9":"cafebabefacedbaddecaf888":"":128:"8d645a0b0e48d3c3b60a014157cb49b4":"FAIL":0

Camellia-GCM test vect draft-kato-ipsec-camellia-gcm #10 (192-bad)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308feffe9928665731c":"0f009e88410d84ad93c90d55efbe20ffa855492f4dfd0fb485c4f02f536feffbb4d967729e5c67f1de0750255cc500716ba483eb3b0a2bf607af28f6":"cafebabefacedbaddecaf888":"feedfacedeadbeeffeedfacedeadbeefabaddad2":128:"11b15bb5ab6fac0c422014e91eacbf2b":"FAIL":0

Camellia-GCM
test vect draft-kato-ipsec-camellia-gcm #11 (192-bad)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308feffe9928665731c":"678b3dcb270faa206dc5f6fbb5014996e86d6f3e35cdcdfeb03b37b9b06ff4ff2682248823bd3c84124dc76af7bde3dd440c228b5efbc795dd80dfb6":"cafebabefacedbad":"feedfacedeadbeeffeedfacedeadbeefabaddad3":128:"f876143d933214a5035ff0bb96ff650b":"FAIL":0

Camellia-GCM test vect draft-kato-ipsec-camellia-gcm #12 (192-bad)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308feffe9928665731c":"9733ea567c3bad2259ccd63ef7012f5de709e50b1fdc31f1a16db02ede1b66f11dcc4d953f2d4d4671587b65882afbf9545fdb6deab22413d091b703":"9313225df88406e555909c5aff5269aa6a7a9538534f7da1e4c303d2a328a728c3c0c95156809539fcf0e2429a6b525416aedbf5a0de6a57a637b39b":"feedfacedeadbeeffeedfacedeadbeefabaddad2":128:"4b72e520b2521e63d240ed5c903216fa":"FAIL":0

Camellia-GCM

test vect draft-kato-ipsec-camellia-gcm #13 (256-bad)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"00000000000000000000000000000000000000000000000000000000000000000000000000000001":"":"00000000000000000000000000":"":128:"9cdb269b5d293bc5db9c55b057d9b591":"FAIL":0

Camellia-GCM test vect draft-kato-ipsec-camellia-gcm #14 (256-bad)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"00000000000000000000000000000000000000000000000000000000000000000000000000000000":"3d4b2cde666761ba5dfb305178e667fb":"00000000000000000000000001":"":128:"284b63bb143c40ce100fb4dea6bb617b":"FAIL":0

Camellia-GCM test vect draft-kato-ipsec-camellia-gcm #15 (256-bad)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308feffe9928665731c6d6a8f9467308308":"ad142c11579dd95e41f3c1f324dabc255864d920f1b65759d8f560d4949d447758dfdcf77aa9f62581c7ff572a037f810cb1a9c4b3ca6ed638179b776549e092":"cafebabefacedbaddecaf888":"":128:"c912686270a2b9966415fca3be75c468":"FAIL":0

Camellia-GCM
test vect draft-kato-ipsec-camellia-gcm #16 (256-bad)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308feffe9928665731c6d6a8f9467308308":"ad142c11579dd95e41f3c1f324dabc255864d920f1b65759d8f560d4948d447758dfdcf77aa9f62581c7ff572a037f810cb1a9c4b3ca6ed638179b77":"cafebabefacedbaddecaf888":"ffedfacedeadbeeffeedfacedeadbeefabaddad2":128:"4e4b178d8fe26fdc95e2e7246dd94bec":"FAIL":0

Camellia-GCM test vect draft-kato-ipsec-camellia-gcm #17 (256-bad)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a8f9467308308feffe9928665731c6d6a8f9467308308":"6ca95fbb7d16577a9ef2fded94dc85b5d40c629f6bef2c649888e3cbb0ededc7810c04b12c2983bbbbc482e16e45c9215ae12c15c55f2f4809d06652":"cafebabefacedbad":"feedfacedeadbeeffeedfacedeadbeefabaddad2":128:"e6472b8ebd331bfcc7c0fa63ce094462":"FAIL":0

Camellia-GCM test vect
draft-kato-ipsec-camellia-gcm #18 (256-bad)
depends_on:MBEDTLS_CAMELLIA_C
gcm_decrypt_and_verify:MBEDTLS_CIPHER_ID_CAMELLIA:"feffe9928665731c6d6a9f9467308308feffe9928665731c6d6a8f9467308308":"e0cddd7564d09c4dc522dd65949262bbf9dcdb07421cf67f3032becb7253c284a16e5bf0f556a308043f53fab9eebb526be7f7ad33d697ac77c67862":"9313225df88406e555909c5aff5269aa6a7a9538534f7da1e4c303d2a318a728c3c0c95156809539fcf0e2429a6b525416aedbf5a0de6a57a637b39b":"feedfacedeadbeeffeedfacedeadbeefabaddad2":128:"5791883f822013f8bd136fc36fb9946b":"FAIL":0
ECP curve info #1
depends_on:MBEDTLS_ECP_DP_BP512R1_ENABLED
mbedtls_ecp_curve_info:MBEDTLS_ECP_DP_BP512R1:28:512:"brainpoolP512r1"

ECP curve info #2
depends_on:MBEDTLS_ECP_DP_BP384R1_ENABLED

mbedtls_ecp_curve_info:MBEDTLS_ECP_DP_BP384R1:27:384:"brainpoolP384r1"

ECP curve info #3
depends_on:MBEDTLS_ECP_DP_BP256R1_ENABLED
mbedtls_ecp_curve_info:MBEDTLS_ECP_DP_BP256R1:26:256:"brainpoolP256r1"

ECP curve info #4
depends_on:MBEDTLS_ECP_DP_SECP521R1_ENABLED
mbedtls_ecp_curve_info:MBEDTLS_ECP_DP_SECP521R1:25:521:"secp521r1"

ECP curve info #5
depends_on:MBEDTLS_ECP_DP_SECP384R1_ENABLED
mbedtls_ecp_curve_info:MBEDTLS_ECP_DP_SECP384R1:24:384:"secp384r1"

ECP curve info #6
depends_on:MBEDTLS_ECP_DP_SECP256R1_ENABLED
mbedtls_ecp_curve_info:MBEDTLS_ECP_DP_SECP256R1:23:256:"secp256r1"

ECP curve info #7
depends_on:MBEDTLS_ECP_DP_SECP224R1_ENABLED
mbedtls_ecp_curve_info:MBEDTLS_ECP_DP_SECP224R1:21:224:"secp224r1"

ECP curve info #8
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
mbedtls_ecp_curve_info:MBEDTLS_ECP_DP_SECP192R1:19:192:"secp192r1"

ECP
check pubkey Montgomery #1 (too big)
depends_on:MBEDTLS_ECP_DP_CURVE25519_ENABLED
ecp_check_pub:MBEDTLS_ECP_DP_CURVE25519:"0100000000000000000000000000000000000000000000000000000000000000":"0":"1":MBEDTLS_ERR_ECP_INVALID_KEY

ECP check pubkey Montgomery #2 (biggest)
depends_on:MBEDTLS_ECP_DP_CURVE25519_ENABLED
ecp_check_pub:MBEDTLS_ECP_DP_CURVE25519:"FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF":"0":"1":0

ECP check pubkey Koblitz #1 (point not on curve)
depends_on:MBEDTLS_ECP_DP_SECP224K1_ENABLED
ecp_check_pub:MBEDTLS_ECP_DP_SECP224K1:"E2000000000000BB3A13D43B323337383935321F0603551D":"100101FF040830060101FF02010A30220603551D0E041B04636FC0C0":"1":MBEDTLS_ERR_ECP_INVALID_KEY

ECP check pubkey Koblitz #2 (coordinate not affine)
depends_on:MBEDTLS_ECP_DP_SECP224K1_ENABLED
ecp_check_pub:MBEDTLS_ECP_DP_SECP224K1:"E2000000000000BB3A13D43B323337383935321F0603551D":"100101FF040830060101FF02010A30220603551D0E041B04636FC0C0":"101":MBEDTLS_ERR_ECP_INVALID_KEY

ECP
write binary #0 (zero, bad format)
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
ecp_write_binary:MBEDTLS_ECP_DP_SECP192R1:"01":"01":"00":ECP_PF_UNKNOWN:"00":1:MBEDTLS_E
RR_ECP_BAD_INPUT_DATA

ECP write binary #1 (zero, uncompressed, buffer just fits)
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
ecp_write_binary:MBEDTLS_ECP_DP_SECP192R1:"01":"01":"00":MBEDTLS_ECP_PF_UNCOMPRESSED:"0
0":1:0

ECP write binary #2 (zero, buffer too small)
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
ecp_write_binary:MBEDTLS_ECP_DP_SECP192R1:"01":"01":"00":MBEDTLS_ECP_PF_UNCOMPRESSED:"0
0":0:MBEDTLS_ERR_ECP_BUFFER_TOO_SMALL

ECP write binary #3 (non-zero, uncompressed, buffer just fits)
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
ecp_write_binary:MBEDTLS_ECP_DP_SECP192R1:"48d8082a3a1e3112bc03a8ef2f6d40d0a77a6f8e00cc9933":"6
ceed4d7cba482e288669ee1b6415626d6f34d28501e060c":"01":MBEDTLS_ECP_PF_UNCOMPRESSED:"0448d8
082a3a1e3112bc03a8ef2f6d40d0a77a6f8e00cc99336ceed4d7cba482e288669ee1b6415626d6f34d28501e060c":49:0

ECP
write binary #4 (non-zero, uncompressed, buffer too small)
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
ecp_write_binary:MBEDTLS_ECP_DP_SECP192R1:"48d8082a3a1e3112bc03a8ef2f6d40d0a77a6f8e00cc9933":"6
ceed4d7cba482e288669ee1b6415626d6f34d28501e060c":"01":MBEDTLS_ECP_PF_UNCOMPRESSED:"0448d8
082a3a1e3112bc03a8ef2f6d40d0a77a6f8e00cc99336ceed4d7cba482e288669ee1b6415626d6f34d28501e060c":48:
MBEDTLS_ERR_ECP_BUFFER_TOO_SMALL

ECP write binary #5 (zero, compressed, buffer just fits)
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
ecp_write_binary:MBEDTLS_ECP_DP_SECP192R1:"01":"01":"00":MBEDTLS_ECP_PF_COMPRESSED:"00":1
:0

ECP write binary #6 (zero, buffer too small)
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
ecp_write_binary:MBEDTLS_ECP_DP_SECP192R1:"01":"01":"00":MBEDTLS_ECP_PF_COMPRESSED:"00":0
:MBEDTLS_ERR_ECP_BUFFER_TOO_SMALL

ECP write binary #7 (even, compressed, buffer just fits)
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
ecp_write_binary:MBEDTLS_ECP_DP_SECP192R1:"48d8082a3a1e3112bc03a8ef2f6d40d0a77a6f8e00cc9933":"6
ceed4d7cba482e288669ee1b6415626d6f34d28501e060c":"01":MBEDTLS_ECP_PF_COMPRESSED:"0248d8082
a3a1e3112bc03a8ef2f6d40d0a77a6f8e00cc9933":25:0

ECP

write binary #8 (even, compressed, buffer too small)
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
ecp_write_binary:MBEDTLS_ECP_DP_SECP192R1:"48d8082a3a1e3112bc03a8ef2f6d40d0a77a6f8e00cc9933":"6ceed4d7cba482e288669ee1b6415626d6f34d28501e060c":"01":MBEDTLS_ECP_PF_COMPRESSED:"0248d8082a3a1e3112bc03a8ef2f6d40d0a77a6f8e00cc9933":24:MBEDTLS_ERR_ECP_BUFFER_TOO_SMALL

ECP write binary #9 (odd, compressed, buffer just fits)
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
ecp_write_binary:MBEDTLS_ECP_DP_SECP192R1:"48d8082a3a1e3112bc03a8ef2f6d40d0a77a6f8e00cc9933":"93112b28345b7d1d7799611e49bea9d8290cb2d7afe1f9f3":"01":MBEDTLS_ECP_PF_COMPRESSED:"0348d8082a3a1e3112bc03a8ef2f6d40d0a77a6f8e00cc9933":25:0

ECP read binary #1 (zero, invalid ilen)
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
ecp_read_binary:MBEDTLS_ECP_DP_SECP192R1:"0000":"01":"01":"00":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECP
read binary #2 (zero, invalid first byte)
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
ecp_read_binary:MBEDTLS_ECP_DP_SECP192R1:"01":"01":"01":"00":MBEDTLS_ERR_ECP_FEATURE_UNAVAILABLE

ECP read binary #3 (zero, OK)
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
ecp_read_binary:MBEDTLS_ECP_DP_SECP192R1:"00":"01":"01":"00":0

ECP read binary #4 (non-zero, invalid ilen)
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
ecp_read_binary:MBEDTLS_ECP_DP_SECP192R1:"04001122":"01":"01":"00":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECP read binary #5 (non-zero, invalid first byte)
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
ecp_read_binary:MBEDTLS_ECP_DP_SECP192R1:"0548d8082a3a1e3112bc03a8ef2f6d40d0a77a6f8e00cc99336ceed4d7cba482e288669ee1b6415626d6f34d28501e060c":"48d8082a3a1e3112bc03a8ef2f6d40d0a77a6f8e00cc9933":"6ceed4d7cba482e288669ee1b6415626d6f34d28501e060c":"01":MBEDTLS_ERR_ECP_FEATURE_UNAVAILABLE

ECP read binary #6 (non-zero,
OK)
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
ecp_read_binary:MBEDTLS_ECP_DP_SECP192R1:"0448d8082a3a1e3112bc03a8ef2f6d40d0a77a6f8e00cc99336ceed4d7cba482e288669ee1b6415626d6f34d28501e060c":"48d8082a3a1e3112bc03a8ef2f6d40d0a77a6f8e00cc9933":"6ceed4d7cba482e288669ee1b6415626d6f34d28501e060c":"01":0

ECP tls read point #1 (zero, invalid length byte)
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED

mbedtls_ecp_tls_read_point:MBEDTLS_ECP_DP_SECP192R1:"0200":"01":"01":"00":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECP tls read point #2 (zero, OK)
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
mbedtls_ecp_tls_read_point:MBEDTLS_ECP_DP_SECP192R1:"0100":"01":"01":"00":0

ECP tls read point #3 (non-zero, invalid length byte)
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
mbedtls_ecp_tls_read_point:MBEDTLS_ECP_DP_SECP192R1:"300448d8082a3a1e3112bc03a8ef2f6d40d0a77a6f8e00cc99336ceed4d7cba482e288669ee1b6415626d6f34d28501e060c":"48d8082a3a1e3112bc03a8ef2f6d40d0a77a6f8e00cc9933":"6ceed4d7cba482e288669ee1b6415626d6f34d28501e060c":"01":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECP
tls read point #4 (non-zero, OK)
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
mbedtls_ecp_tls_read_point:MBEDTLS_ECP_DP_SECP192R1:"310448d8082a3a1e3112bc03a8ef2f6d40d0a77a6f8e00cc99336ceed4d7cba482e288669ee1b6415626d6f34d28501e060c":"48d8082a3a1e3112bc03a8ef2f6d40d0a77a6f8e00cc9933":"6ceed4d7cba482e288669ee1b6415626d6f34d28501e060c":"01":0

ECP tls write-read point #1
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
ecp_tls_write_read_point:MBEDTLS_ECP_DP_SECP192R1

ECP tls write-read point #2
depends_on:MBEDTLS_ECP_DP_SECP521R1_ENABLED
ecp_tls_write_read_point:MBEDTLS_ECP_DP_SECP521R1

ECP tls read group #1 (record too short)
mbedtls_ecp_tls_read_group:"0313":MBEDTLS_ERR_ECP_BAD_INPUT_DATA:0

ECP tls read group #2 (bad curve_type)
mbedtls_ecp_tls_read_group:"010013":MBEDTLS_ERR_ECP_BAD_INPUT_DATA:0

ECP tls read group #3 (unknown curve)
mbedtls_ecp_tls_read_group:"030010":MBEDTLS_ERR_ECP_FEATURE_UNAVAILABLE:0

ECP tls read group #4 (OK, buffer
just fits)
depends_on:MBEDTLS_ECP_DP_SECP256R1_ENABLED
mbedtls_ecp_tls_read_group:"030017":0:256

ECP tls read group #5 (OK, buffer continues)
depends_on:MBEDTLS_ECP_DP_SECP384R1_ENABLED
mbedtls_ecp_tls_read_group:"0300180000":0:384

ECP tls write-read group #1

depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
ecp_tls_write_read_group:MBEDTLS_ECP_DP_SECP192R1

ECP tls write-read group #2
depends_on:MBEDTLS_ECP_DP_SECP521R1_ENABLED
ecp_tls_write_read_group:MBEDTLS_ECP_DP_SECP521R1

ECP check privkey #1 (short weierstrass, too small)
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
mbedtls_ecp_check_privkey:MBEDTLS_ECP_DP_SECP192R1:"00":MBEDTLS_ERR_ECP_INVALID_KEY

ECP check privkey #2 (short weierstrass, smallest)
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
mbedtls_ecp_check_privkey:MBEDTLS_ECP_DP_SECP192R1:"01":0

ECP check privkey #3 (short weierstrass, biggest)
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
mbedtls_ecp_check_privkey:MBEDTLS_ECP_DP_SECP192R1:"FFFFFFFFFFFFFFFFFFFFFFFF99DEF836146B
C9B1B4D22830":0

ECP
check privkey #4 (short weierstrass, too big)
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
mbedtls_ecp_check_privkey:MBEDTLS_ECP_DP_SECP192R1:"FFFFFFFFFFFFFFFFFFFFFFFF99DEF836146B
C9B1B4D22831":MBEDTLS_ERR_ECP_INVALID_KEY

ECP check privkey #5 (montgomery, too big)
depends_on:MBEDTLS_ECP_DP_CURVE25519_ENABLED
mbedtls_ecp_check_privkey:MBEDTLS_ECP_DP_CURVE25519:"C000000000000000000000000000000000000000
0000000000000000000000000":MBEDTLS_ERR_ECP_INVALID_KEY

ECP check privkey #6 (montgomery, not big enough)
depends_on:MBEDTLS_ECP_DP_CURVE25519_ENABLED
mbedtls_ecp_check_privkey:MBEDTLS_ECP_DP_CURVE25519:"3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF0":MBEDTLS_ERR_ECP_INVALID_KEY

ECP check privkey #7 (montgomery, msb OK)
depends_on:MBEDTLS_ECP_DP_CURVE25519_ENABLED
mbedtls_ecp_check_privkey:MBEDTLS_ECP_DP_CURVE25519:"400000000000000000000000000000000000000
0000000000000000000000000":0

ECP check privkey #8 (montgomery, bit 0 set)
depends_on:MBEDTLS_ECP_DP_CURVE25519_ENABLED
mbedtls_ecp_check_privkey:MBEDTLS_ECP_DP_CURVE25519:"400000000000000000000000000000000000000
0000000000000000000000001":MBEDTLS_ERR_ECP_INVALID_KEY

ECP

check privkey #9 (montgomery, bit 1 set)
depends_on:MBEDTLS_ECP_DP_CURVE25519_ENABLED
mbedtls_ecp_check_privkey:MBEDTLS_ECP_DP_CURVE25519:"40000000000000000000000000000000000000000000000000000000000000002":MBEDTLS_ERR_ECP_INVALID_KEY

ECP check privkey #10 (montgomery, bit 2 set)
depends_on:MBEDTLS_ECP_DP_CURVE25519_ENABLED
mbedtls_ecp_check_privkey:MBEDTLS_ECP_DP_CURVE25519:"40000000000000000000000000000000000000000000000000000000000000004":MBEDTLS_ERR_ECP_INVALID_KEY

ECP check privkey #11 (montgomery, OK)
depends_on:MBEDTLS_ECP_DP_CURVE25519_ENABLED
mbedtls_ecp_check_privkey:MBEDTLS_ECP_DP_CURVE25519:"7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF8":0

ECP check public-private #1 (OK)
depends_on:MBEDTLS_ECP_DP_SECP256R1_ENABLED
mbedtls_ecp_check_pub_priv:MBEDTLS_ECP_DP_SECP256R1:"37cc56d976091e5a723ec7592dff206eee7cf9069174d0ad14b5f76822596292":"4ee500d82311ffea2fd2345d5d16bd8a88c26b770d55cd8a2a0efa01c8b4edff":MBEDTLS_ECP_DP_SECP256R1:"00f12a1320760270a83cbffd53f6031ef76a5d86c8a204f2c30ca9ebf51f0f0ea7":"37cc56d976091e5a723ec7592dff206eee7cf9069174d0ad14b5f76822596292":"4ee500d82311ffea2fd2345d5d16bd8a88c26b770d55cd8a2a0efa01c8b4edff":0

ECP
check public-private #2 (group none)
mbedtls_ecp_check_pub_priv:MBEDTLS_ECP_DP_NONE:"37cc56d976091e5a723ec7592dff206eee7cf9069174d0ad14b5f76822596292":"4ee500d82311ffea2fd2345d5d16bd8a88c26b770d55cd8a2a0efa01c8b4edff":MBEDTLS_ECP_DP_NONE:"00f12a1320760270a83cbffd53f6031ef76a5d86c8a204f2c30ca9ebf51f0f0ea7":"37cc56d976091e5a723ec7592dff206eee7cf9069174d0ad14b5f76822596292":"4ee500d82311ffea2fd2345d5d16bd8a88c26b770d55cd8a2a0efa01c8b4edff":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECP check public-private #3 (group mismatch)
depends_on:MBEDTLS_ECP_DP_SECP256R1_ENABLED:MBEDTLS_ECP_DP_SECP384R1_ENABLED
mbedtls_ecp_check_pub_priv:MBEDTLS_ECP_DP_SECP384R1:"37cc56d976091e5a723ec7592dff206eee7cf9069174d0ad14b5f76822596292":"4ee500d82311ffea2fd2345d5d16bd8a88c26b770d55cd8a2a0efa01c8b4edff":MBEDTLS_ECP_DP_SECP256R1:"00f12a1320760270a83cbffd53f6031ef76a5d86c8a204f2c30ca9ebf51f0f0ea7":"37cc56d976091e5a723ec7592dff206eee7cf9069174d0ad14b5f76822596292":"4ee500d82311ffea2fd2345d5d16bd8a88c26b770d55cd8a2a0efa01c8b4edff":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECP
check public-private #4 (Qx mismatch)
depends_on:MBEDTLS_ECP_DP_SECP256R1_ENABLED
mbedtls_ecp_check_pub_priv:MBEDTLS_ECP_DP_SECP256R1:"37cc56d976091e5a723ec7592dff206eee7cf9069174d0ad14b5f76822596293":"4ee500d82311ffea2fd2345d5d16bd8a88c26b770d55cd8a2a0efa01c8b4edff":MBEDTLS_ECP_DP_SECP256R1:"00f12a1320760270a83cbffd53f6031ef76a5d86c8a204f2c30ca9ebf51f0f0ea7":"37cc56d976091e5a723ec7592dff206eee7cf9069174d0ad14b5f76822596292":"4ee500d82311ffea2fd2345d5d16bd8a88c26b770d55cd8a2a0efa01c8b4edff":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECP check public-private #5 (Qy mismatch)
depends_on:MBEDTLS_ECP_DP_SECP256R1_ENABLED
mbedtls_ecp_check_pub_priv:MBEDTLS_ECP_DP_SECP256R1:"37cc56d976091e5a723ec7592dff206eee7cf9069174d0ad14b5f76822596292":"4ee500d82311ffea2fd2345d5d16bd8a88c26b770d55cd8a2a0efa01c8b4edfe":MBEDTLS_ECP_DP_SECP256R1:"00f12a1320760270a83cbffd53f6031ef76a5d86c8a204f2c30ca9ebf51f0f0ea7":"37cc56d976091e5a723ec7592dff206eee7cf9069174d0ad14b5f76822596292":"4ee500d82311ffea2fd2345d5d16bd8a88c26b770d55cd8a2a0efa01c8b4edff":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECP
check public-private #6 (wrong Qx)
depends_on:MBEDTLS_ECP_DP_SECP256R1_ENABLED
mbedtls_ecp_check_pub_priv:MBEDTLS_ECP_DP_SECP256R1:"37cc56d976091e5a723ec7592dff206eee7cf9069174d0ad14b5f76822596293":"4ee500d82311ffea2fd2345d5d16bd8a88c26b770d55cd8a2a0efa01c8b4edff":MBEDTLS_ECP_DP_SECP256R1:"00f12a1320760270a83cbffd53f6031ef76a5d86c8a204f2c30ca9ebf51f0f0ea7":"37cc56d976091e5a723ec7592dff206eee7cf9069174d0ad14b5f76822596293":"4ee500d82311ffea2fd2345d5d16bd8a88c26b770d55cd8a2a0efa01c8b4edff":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECP check public-private
#7 (wrong Qy)
depends_on:MBEDTLS_ECP_DP_SECP256R1_ENABLED
mbedtls_ecp_check_pub_priv:MBEDTLS_ECP_DP_SECP256R1:"37cc56d976091e5a723ec7592dff206eee7cf9069174d0ad14b5f76822596292":"4ee500d82311ffea2fd2345d5d16bd8a88c26b770d55cd8a2a0efa01c8b4edfe":MBEDTLS_ECP_DP_SECP256R1:"00f12a1320760270a83cbffd53f6031ef76a5d86c8a204f2c30ca9ebf51f0f0ea7":"37cc56d976091e5a723ec7592dff206eee7cf9069174d0ad14b5f76822596292":"4ee500d82311ffea2fd2345d5d16bd8a88c26b770d55cd8a2a0efa01c8b4edfe":MBEDTLS_ERR_ECP_BAD_INPUT_DATA

ECP gen keypair
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
mbedtls_ecp_gen_keypair:MBEDTLS_ECP_DP_SECP192R1

ECP gen keypair
depends_on:MBEDTLS_ECP_DP_CURVE25519_ENABLED
mbedtls_ecp_gen_keypair:MBEDTLS_ECP_DP_CURVE25519

ECP gen keypair wrapper
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
mbedtls_ecp_gen_key:MBEDTLS_ECP_DP_SECP192R1

ECP mod p192 small (more than 192 bits, less limbs than 2 * 192 bits)
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
ecp_fast_mod:MBEDTLS_ECP_DP_SECP192R1:"0100000000000103010000000000010201000000000000101010000000000100"

ECP
mod p192 readable
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
ecp_fast_mod:MBEDTLS_ECP_DP_SECP192R1:"0100000000000105010000000000010401000000000000103010000000000102010000000000010101000000000000100"

ECP mod p192 readable with carry
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
ecp_fast_mod:MBEDTLS_ECP_DP_SECP192R1:"FF00000000010500FF00000000010400FF00000000010300FF00000000010200FF00000000010100FF00000000010000"

ECP mod p192 random
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
ecp_fast_mod:MBEDTLS_ECP_DP_SECP192R1:"36CF96B45D706A0954D89E52CE5F38517A2270E0175849B6F3740151D238CCABEF921437E475881D83BB69E4AA258EBD"

ECP mod p192 (from a past failure case)
depends_on:MBEDTLS_ECP_DP_SECP192R1_ENABLED
ecp_fast_mod:MBEDTLS_ECP_DP_SECP192R1:"1AC2D6F96A2A425E9DD1776DD8368D4BBC86BF4964E79FEA713583BF948BBEFF0939F96FB19EC48C585BDA6A2D35C750"

ECP mod p224 readable without carry
depends_on:MBEDTLS_ECP_DP_SECP224R1_ENABLED
ecp_fast_mod:MBEDTLS_ECP_DP_SECP224R1:"0000000D0000000C0000000B0000000A000000090000000800000000070000FF060000FF050000FF040000FF03000FF0020000FF010000FF00"

ECP
mod p224 readable with negative carry
depends_on:MBEDTLS_ECP_DP_SECP224R1_ENABLED
ecp_fast_mod:MBEDTLS_ECP_DP_SECP224R1:"0000000D0000000C0000000B0000000A000000090000000800000000700000006000000050000000400000003000000020000000100000000"

ECP mod p224 readable with positive carry
depends_on:MBEDTLS_ECP_DP_SECP224R1_ENABLED
ecp_fast_mod:MBEDTLS_ECP_DP_SECP224R1:"0000000D0000000C0000000BFFFFFFF0AFFFFFF09FFFFFF08FFFFFF070000FF060000FF050000FF040000FF03000FF0020000FF010000FF00"

ECP mod p224 readable with final negative carry
depends_on:MBEDTLS_ECP_DP_SECP224R1_ENABLED
ecp_fast_mod:MBEDTLS_ECP_DP_SECP224R1:"FF00000D0000000C0000000B0000000A000000090000000800000000700000006000000050000000400000003000000020000000100000000"

ECP mod p521 very small
depends_on:MBEDTLS_ECP_DP_SECP521R1_ENABLED
ecp_fast_mod:MBEDTLS_ECP_DP_SECP521R1:"01"

ECP mod p521 small
(522 bits)
depends_on:MBEDTLS_ECP_DP_SECP521R1_ENABLED
ecp_fast_mod:MBEDTLS_ECP_DP_SECP521R1:"0300000000000

depends_on:MBEDTLS_ECP_DP_SECP521R1_ENABLED
ecp_fast_mod:MBEDTLS_ECP_DP_SECP521R1:"03FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FF0000000000

057AB62F82054D10EE6B0403D6279547E6A8EA9D1FD77427D016FE27A8B8C66":"C6C41294331D23E6F480F4FB4CD40504C947392E94F4C3F06B8F398BB29E42368F7A685923DE3B67BACED214A1A1D128":"52D1791FDB4B70F89C0F00D456C2F7023B6125262C36A7DF1F80231121CCE3D39BE52E00C194A4132C4A6C768BCD94D2":"5CD42AB9C41B5347F74B8D4EFB708B3D5B36DB65915359B44ABC17647B6B9999789D72A84865AE2F223F12B5A1ABC120":"E171458FEAA939AAA3A8BFAC46B404BD8F6D5B348C0FA4D80CECA16356CA933240BDE8723415A8ECE035B0EDF36755DE":"5EA1FC4AF7256D2055981B110575E0A8CAE53160137D904C59D926EB1B8456E427AA8A4540884C37DE159A58028ABC0E":"0CC59E4B046414A81C8A3BDFDCA92526C48769DD8D3127CAA99B3632D1913942DE362EAFAA962379374D9F3F066841CA"

ECP
 test vectors secp521r1 rfc 5114
depends_on:MBEDTLS_ECP_DP_SECP521R1_ENABLED
ecp_test_vect:MBEDTLS_ECP_DP_SECP521R1:"0113F82DA825735E3D97276683B2B74277BAD27335EA71664AF2430CC4F33459B9669EE78B3FFB9B8683015D344DCBFEF6FB9AF4C6C470BE254516CD3C1A1FB47362":"01EBB34DD75721ABF8ADC9DBED17889CBB9765D90A7C60F2CEF007BB0F2B26E14881FD4442E689D61CB2DD046EE30E3FFD20F9A45BBDF6413D583A2DBF59924FD35C":"00F6B632D194C0388E22D8437E558C552AE195ADFD153F92D74908351B2F8C4EDA94EDB0916D1B53C020B5EECAED1A5FC38A233E4830587BB2EE3489B3B42A5A86A4":"00CEE3480D8645A17D249F2776D28BAE616952D1791FDB4B70F7C3378732AA1B22928448BCD1DC2496D435B01048066EBE4F72903C361B1A9DC1193DC2C9D0891B96":"010EBFAFC6E85E08D24BFFFCC1A4511DB0E634BEEB1B6DEC8C5939AE44766201AF6200430BA97C8AC6A0E9F08B33CE7E9FEEB5BA4EE5E0D81510C24295B8A08D0235":"00A4A6EC300DF9E257B0372B5E7ABFEF093436719A77887EBB0B18CF8099B9F4212B6E30A1419C18E029D36863CC9D448F4DBA4D2A0E60711BE572915FBD4FEF2695":"00CDEA89621CFA46B132F9E4CFE2261CDE2D4368EB5656634C7CC98C7A00CDE54ED1866A0DD3E6126C9D2F845DAFF82CEB1DA08F5D87521BB0EBECA77911169C20CC":"00F9A71641029B7FC1A808AD07CD4861E868614B865AFBECAB1F2BD4D8B55EBCB5E3A53143CEB2C511B1AE0AF5AC827F60F2FD872565AC5CA0A164038FE980A7E4BD"

ECP
 test vectors brainpoolP256r1 rfc 7027
depends_on:MBEDTLS_ECP_DP_BP256R1_ENABLED
ecp_test_vect:MBEDTLS_ECP_DP_BP256R1:"81DB1EE100150FF2EA338D708271BE38300CB54241D79950F77B063039804F1D":"44106E913F92BC02A1705D9953A8414DB95E1AAA49E81D9E85F929A8E3100BE5":"8AB4846F11CACCB73CE49CBDD120F5A900A69FD32C272223F789EF10EB089BDC":"55E40BC41E37E3E2AD25C3C6654511FFA8474A91A0032087593852D3E7D76BD3":"8D2D688C6CF93E1160AD04CC4429117DC2C41825E1E9FCA0ADDD34E6F1B39F7B":"990C57520812BE512641E47034832106BC7D3E8DD0E4C7F1136D7006547CEC6A":"89AFC39D41D3B327814B80940B042590F96556EC91E6AE7939BCE31F3A18BF2B":"49C27868F4ECA2179BFD7D59B1E3BF34C1DBDE61AE12931648F43E59632504DE"

ECP
 test vectors brainpoolP384r1 rfc 7027
depends_on:MBEDTLS_ECP_DP_BP384R1_ENABLED
ecp_test_vect:MBEDTLS_ECP_DP_BP384R1:"1E20F5E048A5886F1F157C74E91BDE2B98C8B52D58E5003D57053FC4B0BD65D6F15EB5D1EE1610DF870795143627D042":"68B665DD91C195800650CDD363C625F4E742E8134667B767B1B476793588F885AB698C852D4A6E77A252D6380FCAF068":"55BC91A39C9EC01DEE36017B7D673A931236D2F1F5C83942D049E3FA20607493E0D038FF2FD30C2AB67D15C85F7FAA59":"032640BC6003C59260F7250C3DB58CE647F98E1260ACCE4ACDA3DD869F74E01F8BA5E0324309DB6A9831497ABAC96670":"4D44326F269A597A5B58BBA565DA5556ED7FD9A8A9EB76C25F46DB69D19DC8CE6AD18E404B15738B2086DF37E71D1EB4":"62D692136DE56CBE93BF5FA3188EF58BC8A3A0EC6C1E151A21038A42E91853

29B5B275903D192F8D4E1F32FE9CC78C48":"0BD9D3A7EA0B3D519D09D8E48D0785FB744A6B355E6304B
C51C229FBBCE239BBADF6403715C35D4FB2A5444F575D4F42":"0DF213417EBE4D8E40A5F76F66C56470C
489A3478D146DECF6DF0D94BAE9E598157290F8756066975F1DB34B2324B7BD"

ECP
test vectors brainpoolP512r1 rfc 7027
depends_on:MBEDTLS_ECP_DP_BP512R1_ENABLED
ecp_test_vect:MBEDTLS_ECP_DP_BP512R1:"16302FF0DBBB5A8D733DAB7141C1B45ACBC8715939677F6
A56850A38BD87BD59B09E80279609FF333EB9D4C061231FB26F92EEB04982A5F1D1764CAD57665422":"0
A420517E406AAC0ACDCE90FCD71487718D3B953EFD7FBEC5F7F27E28C6149999397E91E029E06457DB2
D3E640668B392C2A7E737A7F0BF04436D11640FD09FD":"72E6882E8DB28AAD36237CD25D580DB2378396
1C8DC52DFA2EC138AD472A0FCEF3887CF62B623B2A87DE5C588301EA3E5FC269B373B60724F5E82A6A
D147FDE7":"230E18E1BCC88A362FA54E4EA3902009292F7F8033624FD471B5D8ACE49D12CFABBC19963
DAB8E2F1EBA00BFFB29E4D72D13F2224562F405CB80503666B25429":"9D45F66DE5D67E2E6DB6E93A59
CE0BB48106097FF78A081DE781CDB31FCE8CCBAAEA8DD4320C4119F1E9CD437A2EAB3731FA9668AB2
68D871DEDA55A5473199F":"2FDC313095BCDD5FB3A91636F07A959C8E86B5636A1E930E8396049CB4819
61D365CC11453A06C719835475B12CB52FC3C383BCE35E27EF194512B71876285FA":"A7927098655F1F997
6FA50A9D566865DC530331846381C87256BAF3226244B76D36403C024D7BBF0AA0803EAFF405D3D24F11
A9B5C0BEF679FE1454B21C4CD1F":"7DB71C3DEF63212841C463E881BDCF055523BD368240E6C3143BD8
DEF8B3B3223B95E0F53082FF5E412F4222537A43DF1C6D25729DDB51620A832BE6A26680A2"

ECP
test vectors Curve25519
depends_on:MBEDTLS_ECP_DP_CURVE25519_ENABLED
ecp_test_vec_x:MBEDTLS_ECP_DP_CURVE25519:"5AC99F33632E5A768DE7E81BF854C27C46E3FBF2ABB
ACD29EC4AFF517369C660":"057E23EA9F1CBE8A27168F6E696A791DE61DD3AF7ACD4EEACC6E7BA514
FDA863":"47DC3D214174820E1154B49BC6CDB2ABD45EE95817055D255AA35831B70D3260":"6EB89DA91
989AE37C7EAC7618D9E5C4951DBA1D73C285AE1CD26A855020EEF04":"61450CD98E36016B58776A897A
9F0AEF738B99F09468B8D6B8511184D53494AB"

ECP
test vectors secp192k1
depends_on:MBEDTLS_ECP_DP_SECP192K1_ENABLED
ecp_test_vect:MBEDTLS_ECP_DP_SECP192K1:"D1E13A359F6E0F0698791938E6D60246030AE4B0D8D4E9D
E":"281BCA982F187ED30AD5E088461EBE0A5FADBB682546DF79":"3F68A8E9441FB93A4DD48CB70B504
FCC9AA01902EF5BE0F3":"BE97C5D2A1A94D081E3FACE53E65A27108B7467BDF58DE43":"5EB35E922CD
693F7947124F5920022C4891C04F6A8B8DCB2":"60ECF73D0FC43E0C42E8E155FFE39F9F0B531F87B34B6C
3C":"372F5C5D0E18313C82AEF940EC3AFEE26087A46F1EBAE923":"D5A9F9182EC09CEAEA5F57EA10225
EC77FA44174511985FD"

ECP test vectors secp224k1
depends_on:MBEDTLS_ECP_DP_SECP224K1_ENABLED
ecp_test_vect:MBEDTLS_ECP_DP_SECP224K1:"8EAD9B2819A3C2746B3EDC1E0D30F23271CDAC048C061
5C961B1A9D3":"DEE0A75EF26CF8F501DB80807A3A0908E5CF01852709C1D35B31428B":"276D2B817918F
7CD1DA5CCA081EC4B62CD255E0ACDC9F85FA8C52CAC":"AB7E70AEDA68A174ECC1F3800561B2D4FA
BE97C5D2A1A94D081E3FAC":"D2E94B00FD30201C40EDF73B137427916687AEA1935B277A5960DD1C":"
DE728A614B17D91EB3CB2C17DA195562B6281585986332B3E12DA0ED":"B66B673D29038A3487A2D9C10
CDCE67646F7C39C984EBE9E8795AD3C":"928C6147AF5EE4B54FA6ECF77B70CA3FEE5F4182DB057878F1

29DF":

ECP
test vectors secp256k1
depends_on:MBEDTLS_ECP_DP_SECP256K1_ENABLED
ecp_test_vect:MBEDTLS_ECP_DP_SECP256K1:"923C6D4756CD940CD1E13A359F6E0F0698791938E6D6024
6030AE4B0D8D4E9DE":"20A865B295E93C5B090F324B84D7AC7526AA1CFE86DD80E792CECCD16B657D5
5":"38AC87141A4854A8DFD87333E107B61692323721FE2EAD6E52206FE471A4771B":"4F5036A8ED5809AB
7E70AEDA68A174ECC1F3800561B2D4FABE97C5D2A1A94D08":"029F5D2CC5A2C7E538FBA321439B4EC8
DD79B7FEB9C0A8A5114EEA39856E22E8":"165171AFC3411A427F24FDDE1192A551C90983EB421BC982A
B4CF4E21F18F04B":"E4B5B537D3ACEA7624F2E9C185BFFD80BC7035E515F33E0D4CFAE747FD20038E":"
2BC685B7DCDBC694F5E036C4EAE9BFB489D7BF8940C4681F734B71D68501514C"

ECP selftest
ecp_selftest:
CAMELLIA Encrypt and decrypt 0 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:0:-1

CAMELLIA Encrypt and decrypt 1 byte
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:1:-1

CAMELLIA Encrypt and decrypt 2 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:2:-1

CAMELLIA Encrypt and decrypt 7 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:7:-1

CAMELLIA Encrypt and decrypt 8 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:8:-1

CAMELLIA Encrypt and decrypt 9 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:9:-1

CAMELLIA
Encrypt and decrypt 15 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P

KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:15:-1

CAMELLIA Encrypt and decrypt 16 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:16:-1

CAMELLIA Encrypt and decrypt 17 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:17:-1

CAMELLIA Encrypt and decrypt 31 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:31:-1

CAMELLIA Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:32:-1

CAMELLIA
Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:33:-1

CAMELLIA Encrypt and decrypt 47 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:47:-1

CAMELLIA Encrypt and decrypt 48 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:48:-1

CAMELLIA Encrypt and decrypt 49 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:49:-1

CAMELLIA Encrypt and decrypt 0 bytes with one and zeros padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-

CBC":128:0:MBEDTLS_PADDING_ONE_AND_ZEROS

CAMELLIA
Encrypt and decrypt 1 byte with one and zeros padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:1:MBEDTLS_PADDING_ONE_AND_ZEROS

CAMELLIA Encrypt and decrypt 2 bytes with one and zeros padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:2:MBEDTLS_PADDING_ONE_AND_ZEROS

CAMELLIA Encrypt and decrypt 7 bytes with one and zeros padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:7:MBEDTLS_PADDING_ONE_AND_ZEROS

CAMELLIA Encrypt and decrypt 8 bytes with one and zeros padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:8:MBEDTLS_PADDING_ONE_AND_ZEROS

CAMELLIA
Encrypt and decrypt 9 bytes with one and zeros padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:9:MBEDTLS_PADDING_ONE_AND_ZEROS

CAMELLIA Encrypt and decrypt 15 bytes with one and zeros padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:15:MBEDTLS_PADDING_ONE_AND_ZEROS

CAMELLIA Encrypt and decrypt 16 bytes with one and zeros padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:16:MBEDTLS_PADDING_ONE_AND_ZEROS

CAMELLIA Encrypt and decrypt 17 bytes with one and zeros padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P

KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-
CBC":128:17:MBEDTLS_PADDING_ONE_AND_ZEROS

CAMELLIA
Encrypt and decrypt 31 bytes with one and zeros padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-
CBC":128:31:MBEDTLS_PADDING_ONE_AND_ZEROS

CAMELLIA Encrypt and decrypt 32 bytes with one and zeros padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-
CBC":128:32:MBEDTLS_PADDING_ONE_AND_ZEROS

CAMELLIA Encrypt and decrypt 32 bytes with one and zeros padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-
CBC":128:33:MBEDTLS_PADDING_ONE_AND_ZEROS

CAMELLIA Encrypt and decrypt 47 bytes with one and zeros padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-
CBC":128:47:MBEDTLS_PADDING_ONE_AND_ZEROS

CAMELLIA
Encrypt and decrypt 48 bytes with one and zeros padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-
CBC":128:48:MBEDTLS_PADDING_ONE_AND_ZEROS

CAMELLIA Encrypt and decrypt 49 bytes with one and zeros padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-
CBC":128:49:MBEDTLS_PADDING_ONE_AND_ZEROS

CAMELLIA Encrypt and decrypt 0 bytes with zeros and len padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-
CBC":128:0:MBEDTLS_PADDING_ZEROS_AND_LEN

CAMELLIA Encrypt and decrypt 1 byte with zeros and len padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:1:MBEDTLS_PADDING_ZEROS_AND_LEN

CAMELLIA
Encrypt and decrypt 2 bytes with zeros and len padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:2:MBEDTLS_PADDING_ZEROS_AND_LEN

CAMELLIA Encrypt and decrypt 7 bytes with zeros and len padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:7:MBEDTLS_PADDING_ZEROS_AND_LEN

CAMELLIA Encrypt and decrypt 8 bytes with zeros and len padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:8:MBEDTLS_PADDING_ZEROS_AND_LEN

CAMELLIA Encrypt and decrypt 9 bytes with zeros and len padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:9:MBEDTLS_PADDING_ZEROS_AND_LEN

CAMELLIA
Encrypt and decrypt 15 bytes with zeros and len padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:15:MBEDTLS_PADDING_ZEROS_AND_LEN

CAMELLIA Encrypt and decrypt 16 bytes with zeros and len padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:16:MBEDTLS_PADDING_ZEROS_AND_LEN

CAMELLIA Encrypt and decrypt 17 bytes with zeros and len padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-

CBC":128:17:MBEDTLS_PADDING_ZEROS_AND_LEN

CAMELLIA Encrypt and decrypt 31 bytes with zeros and len padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:31:MBEDTLS_PADDING_ZEROS_AND_LEN

CAMELLIA
Encrypt and decrypt 32 bytes with zeros and len padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:32:MBEDTLS_PADDING_ZEROS_AND_LEN

CAMELLIA Encrypt and decrypt 32 bytes with zeros and len padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:33:MBEDTLS_PADDING_ZEROS_AND_LEN

CAMELLIA Encrypt and decrypt 47 bytes with zeros and len padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:47:MBEDTLS_PADDING_ZEROS_AND_LEN

CAMELLIA Encrypt and decrypt 48 bytes with zeros and len padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:48:MBEDTLS_PADDING_ZEROS_AND_LEN

CAMELLIA
Encrypt and decrypt 49 bytes with zeros and len padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:49:MBEDTLS_PADDING_ZEROS_AND_LEN

CAMELLIA Encrypt and decrypt 0 bytes with zeros padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:0:MBEDTLS_PADDING_ZEROS

CAMELLIA Encrypt and decrypt 1 byte with zeros padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P

KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-
CBC":128:1:MBEDTLS_PADDING_ZEROS

CAMELLIA Encrypt and decrypt 2 bytes with zeros padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-
CBC":128:2:MBEDTLS_PADDING_ZEROS

CAMELLIA
Encrypt and decrypt 7 bytes with zeros padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-
CBC":128:7:MBEDTLS_PADDING_ZEROS

CAMELLIA Encrypt and decrypt 8 bytes with zeros padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-
CBC":128:8:MBEDTLS_PADDING_ZEROS

CAMELLIA Encrypt and decrypt 9 bytes with zeros padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-
CBC":128:9:MBEDTLS_PADDING_ZEROS

CAMELLIA Encrypt and decrypt 15 bytes with zeros padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-
CBC":128:15:MBEDTLS_PADDING_ZEROS

CAMELLIA Encrypt and decrypt
16 bytes with zeros padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-
CBC":128:16:MBEDTLS_PADDING_ZEROS

CAMELLIA Encrypt and decrypt 17 bytes with zeros padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P
KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-
CBC":128:17:MBEDTLS_PADDING_ZEROS

CAMELLIA Encrypt and decrypt 31 bytes with zeros padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:31:MBEDTLS_PADDING_ZEROS

CAMELLIA Encrypt and decrypt 32 bytes with zeros padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:32:MBEDTLS_PADDING_ZEROS

CAMELLIA Encrypt and decrypt 32 bytes with zeros padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:33:MBEDTLS_PADDING_ZEROS

CAMELLIA
Encrypt and decrypt 47 bytes with zeros padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:47:MBEDTLS_PADDING_ZEROS

CAMELLIA Encrypt and decrypt 48 bytes with zeros padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:48:MBEDTLS_PADDING_ZEROS

CAMELLIA Encrypt and decrypt 49 bytes with zeros padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:49:MBEDTLS_PADDING_ZEROS

CAMELLIA Encrypt and decrypt 0 bytes with no padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:0:MBEDTLS_PADDING_NONE

CAMELLIA
Encrypt and decrypt 16 bytes with no padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-

CBC":128:16:MBEDTLS_PADDING_NONE

CAMELLIA Encrypt and decrypt 32 bytes with no padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:32:MBEDTLS_PADDING_NONE

CAMELLIA Encrypt and decrypt 48 bytes with no padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CBC:"CAMELLIA-128-CBC":128:48:MBEDTLS_PADDING_NONE

CAMELLIA Try encrypting 1 bytes with no padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_CAMELLIA_128_CBC:MBEDTLS_PADDING_NONE:128:1:MBEDTLS_ERR_CIPHER_FULL_BLOCK_EXPECTED

CAMELLIA Try
encrypting 2 bytes with no padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_CAMELLIA_128_CBC:MBEDTLS_PADDING_NONE:128:2:MBEDTLS_ERR_CIPHER_FULL_BLOCK_EXPECTED

CAMELLIA Try encrypting 7 bytes with no padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_CAMELLIA_128_CBC:MBEDTLS_PADDING_NONE:128:7:MBEDTLS_ERR_CIPHER_FULL_BLOCK_EXPECTED

CAMELLIA Try encrypting 8 bytes with no padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_CAMELLIA_128_CBC:MBEDTLS_PADDING_NONE:128:8:MBEDTLS_ERR_CIPHER_FULL_BLOCK_EXPECTED

CAMELLIA Try encrypting 9 bytes with no padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_CAMELLIA_128_CBC:MBEDTLS_PADDING_NONE:128:9:MBEDTLS_ERR_CIPHER_FULL_BLOCK_EXPECTED

CAMELLIA Try encrypting 15 bytes with no padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7

enc_fail:MBEDTLS_CIPHER_CAMELLIA_128_CBC:MBEDTLS_PADDING_NONE:128:15:MBEDTLS_ERR_CIPHER_FULL_BLOCK_EXPECTED

CAMELLIA
Try encrypting 17 bytes with no padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_CAMELLIA_128_CBC:MBEDTLS_PADDING_NONE:128:17:MBEDTLS_ERR_CIPHER_FULL_BLOCK_EXPECTED

CAMELLIA Try encrypting 31 bytes with no padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_CAMELLIA_128_CBC:MBEDTLS_PADDING_NONE:128:31:MBEDTLS_ERR_CIPHER_FULL_BLOCK_EXPECTED

CAMELLIA Try encrypting 33 bytes with no padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_CAMELLIA_128_CBC:MBEDTLS_PADDING_NONE:128:33:MBEDTLS_ERR_CIPHER_FULL_BLOCK_EXPECTED

CAMELLIA Try encrypting 47 bytes with no padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_CAMELLIA_128_CBC:MBEDTLS_PADDING_NONE:128:47:MBEDTLS_ERR_CIPHER_FULL_BLOCK_EXPECTED

CAMELLIA
Try encrypting 49 bytes with no padding
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_fail:MBEDTLS_CIPHER_CAMELLIA_128_CBC:MBEDTLS_PADDING_NONE:128:49:MBEDTLS_ERR_CIPHER_FULL_BLOCK_EXPECTED

CAMELLIA Encrypt and decrypt 0 bytes in multiple parts
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CBC:128:0:0:

CAMELLIA Encrypt and decrypt 1 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CBC:128:1:0:

CAMELLIA Encrypt and decrypt 1 bytes in multiple parts 2
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7

enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CBC:128:0:1:

CAMELLIA
Encrypt and decrypt 16 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CBC:128:16:0:

CAMELLIA Encrypt and decrypt 16 bytes in multiple parts 2
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CBC:128:0:16:

CAMELLIA Encrypt and decrypt 16 bytes in multiple parts 3
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CBC:128:1:15:

CAMELLIA Encrypt and decrypt 16 bytes in multiple parts 4
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CBC:128:15:1:

CAMELLIA Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CBC:128:15:7:

CAMELLIA
Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CBC:128:16:6:

CAMELLIA Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CBC:128:17:6:

CAMELLIA Encrypt and decrypt 32 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CBC:128:16:16:

CAMELLIA Encrypt and decrypt 0 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CFB128:"CAMELLIA-128-CFB128":128:0:-1

CAMELLIA Encrypt and decrypt 1 byte
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CFB128:"CAMELLIA-128-CFB128":128:1:-1

CAMELLIA Encrypt
and decrypt 2 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CFB128:"CAMELLIA-128-CFB128":128:2:-1

CAMELLIA Encrypt and decrypt 7 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CFB128:"CAMELLIA-128-CFB128":128:7:-1

CAMELLIA Encrypt and decrypt 8 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CFB128:"CAMELLIA-128-CFB128":128:8:-1

CAMELLIA Encrypt and decrypt 9 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CFB128:"CAMELLIA-128-CFB128":128:9:-1

CAMELLIA Encrypt and decrypt 15 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CFB128:"CAMELLIA-128-CFB128":128:15:-1

CAMELLIA Encrypt and decrypt 16 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CFB128:"CAMELLIA-128-CFB128":128:16:-1

CAMELLIA
Encrypt and decrypt 17 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CFB128:"CAMELLIA-128-CFB128":128:17:-1

CAMELLIA Encrypt and decrypt 31 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CFB128:"CAMELLIA-128-CFB128":128:31:-1

CAMELLIA Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CFB128:"CAMELLIA-128-CFB128":128:32:-1

CAMELLIA Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CFB128:"CAMELLIA-128-CFB128":128:33:-1

CAMELLIA Encrypt and decrypt 47 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CFB

enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CFB128:"CAMELLIA-128-CFB128":128:47:-1

CAMELLIA Encrypt and decrypt 48 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CFB128:"CAMELLIA-128-CFB128":128:48:-1

CAMELLIA
Encrypt and decrypt 49 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CFB128:"CAMELLIA-128-CFB128":128:49:-1

CAMELLIA Encrypt and decrypt 0 bytes in multiple parts
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CFB128:128:0:0:

CAMELLIA Encrypt and decrypt 1 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CFB128:128:1:0:

CAMELLIA Encrypt and decrypt 1 bytes in multiple parts 2
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CFB128:128:0:1:

CAMELLIA Encrypt and decrypt 16 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CFB128:128:16:0:

CAMELLIA Encrypt and decrypt 16 bytes in multiple parts 2
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CFB128:128:0:16:

CAMELLIA
Encrypt and decrypt 16 bytes in multiple parts 3
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CFB128:128:1:15:

CAMELLIA Encrypt and decrypt 16 bytes in multiple parts 4
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CFB128:128:15:1:

CAMELLIA Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CFB128:128:15:7:

CAMELLIA Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CFB128:128:16:6:

CAMELLIA Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CFB128:128:17:6:

CAMELLIA
Encrypt and decrypt 32 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CFB
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CFB128:128:16:16:

CAMELLIA Encrypt and decrypt 0 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CTR:"CAMELLIA-128-CTR":128:0:-1

CAMELLIA Encrypt and decrypt 1 byte
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CTR:"CAMELLIA-128-CTR":128:1:-1

CAMELLIA Encrypt and decrypt 2 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CTR:"CAMELLIA-128-CTR":128:2:-1

CAMELLIA Encrypt and decrypt 7 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CTR:"CAMELLIA-128-CTR":128:7:-1

CAMELLIA Encrypt and decrypt 8 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CTR:"CAMELLIA-128-CTR":128:8:-1

CAMELLIA
Encrypt and decrypt 9 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CTR:"CAMELLIA-128-CTR":128:9:-1

CAMELLIA Encrypt and decrypt 15 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CTR:"CAMELLIA-128-CTR":128:15:-1

CAMELLIA Encrypt and decrypt 16 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CTR:"CAMELLIA-128-CTR":128:16:-1

CAMELLIA Encrypt and decrypt 17 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CTR:"CAMELLIA-128-CTR":128:17:-1

CAMELLIA Encrypt and decrypt 31 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CTR

enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CTR:"CAMELLIA-128-CTR":128:31:-1

CAMELLIA Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CTR:"CAMELLIA-128-CTR":128:32:-1

CAMELLIA
Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CTR:"CAMELLIA-128-CTR":128:33:-1

CAMELLIA Encrypt and decrypt 47 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CTR:"CAMELLIA-128-CTR":128:47:-1

CAMELLIA Encrypt and decrypt 48 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CTR:"CAMELLIA-128-CTR":128:48:-1

CAMELLIA Encrypt and decrypt 49 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_128_CTR:"CAMELLIA-128-CTR":128:49:-1

CAMELLIA Encrypt and decrypt 0 bytes in multiple parts
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CTR:128:0:0:

CAMELLIA Encrypt and decrypt 1 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CTR:128:1:0:

CAMELLIA
Encrypt and decrypt 1 bytes in multiple parts 2
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CTR:128:0:1:

CAMELLIA Encrypt and decrypt 16 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CTR:128:16:0:

CAMELLIA Encrypt and decrypt 16 bytes in multiple parts 2
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CTR:128:0:16:

CAMELLIA Encrypt and decrypt 16 bytes in multiple parts 3
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CTR:128:1:15:

CAMELLIA Encrypt and decrypt 16 bytes in multiple parts 4
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CTR:128:15:1:

CAMELLIA Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CTR:128:15:7:

CAMELLIA
Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CTR:128:16:6:

CAMELLIA Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CTR:128:17:6:

CAMELLIA Encrypt and decrypt 32 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CTR
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_128_CTR:128:16:16:

CAMELLIA Encrypt and decrypt 0 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_192_CBC:"CAMELLIA-192-CBC":192:0:-1

CAMELLIA Encrypt and decrypt 1 byte
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_192_CBC:"CAMELLIA-192-CBC":192:1:-1

CAMELLIA
Encrypt and decrypt 2 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_192_CBC:"CAMELLIA-192-CBC":192:2:-1

CAMELLIA Encrypt and decrypt 7 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_192_CBC:"CAMELLIA-192-CBC":192:7:-1

CAMELLIA Encrypt and decrypt 8 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_192_CBC:"CAMELLIA-192-CBC":192:8:-1

CAMELLIA Encrypt and decrypt 9 bytes

depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_192_CBC:"CAMELLIA-192-CBC":192:9:-1

CAMELLIA Encrypt and decrypt 15 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_192_CBC:"CAMELLIA-192-CBC":192:15:-1

CAMELLIA Encrypt and decrypt 16 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_192_CBC:"CAMELLIA-192-CBC":192:16:-1

CAMELLIA
Encrypt and decrypt 17 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_192_CBC:"CAMELLIA-192-CBC":192:17:-1

CAMELLIA Encrypt and decrypt 31 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_192_CBC:"CAMELLIA-192-CBC":192:31:-1

CAMELLIA Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_192_CBC:"CAMELLIA-192-CBC":192:32:-1

CAMELLIA Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_192_CBC:"CAMELLIA-192-CBC":192:33:-1

CAMELLIA Encrypt and decrypt 47 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_192_CBC:"CAMELLIA-192-CBC":192:47:-1

CAMELLIA
Encrypt and decrypt 48 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_192_CBC:"CAMELLIA-192-CBC":192:48:-1

CAMELLIA Encrypt and decrypt 49 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P

KCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_192_CBC:"CAMELLIA-192-CBC":192:49:-1

CAMELLIA Encrypt and decrypt 0 bytes in multiple parts
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_192_CBC:192:0:0:

CAMELLIA Encrypt and decrypt 1 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_192_CBC:192:1:0:

CAMELLIA Encrypt and decrypt 1 bytes in multiple parts 2
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_192_CBC:192:0:1:

CAMELLIA
Encrypt and decrypt 16 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_192_CBC:192:16:0:

CAMELLIA Encrypt and decrypt 16 bytes in multiple parts 2
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_192_CBC:192:0:16:

CAMELLIA Encrypt and decrypt 16 bytes in multiple parts 3
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_192_CBC:192:1:15:

CAMELLIA Encrypt and decrypt 16 bytes in multiple parts 4
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_192_CBC:192:15:1:

CAMELLIA Encrypt and decrypt 22 bytes in multiple
parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_192_CBC:192:15:7:

CAMELLIA Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7

enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_192_CBC:192:16:6:

CAMELLIA Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_192_CBC:192:17:6:

CAMELLIA Encrypt and decrypt 32 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_192_CBC:192:16:16:

CAMELLIA Encrypt and decrypt 0 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_256_CBC:"CAMELLIA-256-CBC":256:0:-1

CAMELLIA Encrypt and decrypt
1 byte
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_256_CBC:"CAMELLIA-256-CBC":256:1:-1

CAMELLIA Encrypt and decrypt 2 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_256_CBC:"CAMELLIA-256-CBC":256:2:-1

CAMELLIA Encrypt and decrypt 7 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_256_CBC:"CAMELLIA-256-CBC":256:7:-1

CAMELLIA Encrypt and decrypt 8 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_256_CBC:"CAMELLIA-256-CBC":256:8:-1

CAMELLIA Encrypt and decrypt 9 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_256_CBC:"CAMELLIA-256-CBC":256:9:-1

CAMELLIA Encrypt and decrypt 15 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_256_CBC:"CAMELLIA-256-CBC":256:15:-1

CAMELLIA
Encrypt and decrypt 16 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_256_CBC:"CAMELLIA-256-CBC":256:16:-1

CAMELLIA Encrypt and decrypt 17 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_256_CBC:"CAMELLIA-256-CBC":256:17:-1

CAMELLIA Encrypt and decrypt 31 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_256_CBC:"CAMELLIA-256-CBC":256:31:-1

CAMELLIA Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_256_CBC:"CAMELLIA-256-CBC":256:32:-1

CAMELLIA Encrypt and decrypt 32 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_256_CBC:"CAMELLIA-256-CBC":256:33:-1

CAMELLIA
Encrypt and decrypt 47 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_256_CBC:"CAMELLIA-256-CBC":256:47:-1

CAMELLIA Encrypt and decrypt 48 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_256_CBC:"CAMELLIA-256-CBC":256:48:-1

CAMELLIA Encrypt and decrypt 49 bytes
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf:MBEDTLS_CIPHER_CAMELLIA_256_CBC:"CAMELLIA-256-CBC":256:49:-1

CAMELLIA Encrypt and decrypt 0 bytes in multiple parts
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_256_CBC:256:0:0:

CAMELLIA Encrypt and decrypt 1 bytes in multiple parts 1

depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_256_CBC:256:1:0:

CAMELLIA
Encrypt and decrypt 1 bytes in multiple parts 2
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_256_CBC:256:0:1:

CAMELLIA Encrypt and decrypt 16 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_256_CBC:256:16:0:

CAMELLIA Encrypt and decrypt 16 bytes in multiple parts 2
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_256_CBC:256:0:16:

CAMELLIA Encrypt and decrypt 16 bytes in multiple parts 3
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_256_CBC:256:1:15:

CAMELLIA Encrypt and decrypt 16 bytes in multiple parts 4
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_256_CBC:256:15:1:

CAMELLIA
Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_256_CBC:256:15:7:

CAMELLIA Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_256_CBC:256:16:6:

CAMELLIA Encrypt and decrypt 22 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_PKCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_256_CBC:256:17:6:

CAMELLIA Encrypt and decrypt 32 bytes in multiple parts 1
depends_on:MBEDTLS_CAMELLIA_C:MBEDTLS_CIPHER_MODE_CBC:MBEDTLS_CIPHER_PADDING_P

KCS7
enc_dec_buf_multipart:MBEDTLS_CIPHER_CAMELLIA_256_CBC:256:16:16:
0
10 *H
00 *H
00} *H
0
*H
0?s=\P}{;Jw!]%sRH?AfAoG-
fsCAo_344qwRXrc}4RA~kk^uHZ|h3Ia3Y"=TW"#ThIK(yxT8b}TzBkA]{N!H_A+c%n2Y,/Wwn:wvk~*&O^Q3F
C6pZY0O17zN_MzU"5J:kN5A)!x
y0ZtDqx
IWq8O48Y&f(,C,BR:!!^#+DF
8>f=<u?oG@Fg%^pU1};2E(<u20w

$e5RHeopLeg`eJ=v*+G?1_TG
Y*3gX&hP&^BUdtxX4%65Pyl:kPNWP*B
(G"|y}
0Hub}~O^oa$1Fd2awKr+n{CL`~QDF#)TC=}9wE1;"_D3 =\|tVVg @%^D"aKWJ.b-S^
?P>DF&anIHfA`n(NI_D&/|L6R7X,;N.[Av#$c=H3z3,mOdQ\4k}.]
C]!a,]XxfdI[la1V+7=>`c^[StxA0t2`Ycw9
udtQ`M/6%&1R6\pCaMj ZRoUTBho"VAj(0.H85<XvQ5&;-hv 4
~)+Qju{pFy^mrIh$Do(lpn'oquBIY@Gomd.{ISo49w6#BEA$GCGUVRqGlf}oDb`+ck6{UmSdM4D5wHI<4uDi*u
>r-xQDzf@<8@%}?yrH$lcd/4[6EzxIS7K?xre2"UCEZH8*<w'_mgy@T
Jv74J4a,g|8?+;Zl819&WqIn%A*5qmYA{PqcJGTdTNi\~72yMsi?a_^,Ms.a}~r8 n>H3,'+F,R*-I9?4y}`u"g-
X:9=2HyUpRwZb&f7NJt;]__C;
vz[*Y~0A *H
2.0*0&*H
00
*H
0g]h$crZ-Sn
>`.;lXPu\xu
fxz'pE
MOFzxd(RbxIDhk~#:%=ZwcSULUkS%j@N@6MOrp]pbp
J0]y6> a_pg2fPt6.K*l-V B37 5g8eP5,kJ
,ZbK+N9>Z.vP]'E$K{Z1m\5=:>6Qd7PQ2*.5{"k;bc|/Os!\
o1+aQCM3GcH~8r5|Eazx
l8vvdgkdjL6sZ*&faLb?)#*vkN|IV/(MqG7P/f~X>yY;6h'fO`k^gDNmx`pwc
(RZ?E
CX05K[}F_
?&caK&{pH4e.J`13]9j%j,9^|GnPBc5:?XItSkuM}
=$,rAhS&)-M$#+=^_t)JFV]R|ieI,xD9W*>W2wI7t{IY!S3r$)Mb\ELRXV"*iJ0`}(o&7
W-G,_st@]S3f;p&mo$<zx~!Duk"wE~)$C~6v*Il#=Y\pn7\[56b~iI>Da'X@-QD"~ExsL)1*?".V8RG'
_=366`)IG71%0# *H
1f5Q<4(Y&|010!0 +RNxy8M"!9I5
-----BEGIN CERTIFICATE-----
MIIDFzCCAf+gAwIBAgIBATANBgkqhkiG9w0BAQsFADAmMSQwIgYDVQQDExtUZXN0
IGludGVybWVkaWF0ZSBtYXhwYXRoIDEwHhcNMDEwMTAxMDAwMDAwWhcNMzAxMjMx

MjM1OTU5WjAmMSQwIgYDVQQDExtUZXN0IGludGVybWVkaWF0ZSBtYXhwYXRoIDIw
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCKAaAcY1Y2QRZYWft5pTiQ
LZaNHdG1wGyhbUyVCd1S/BZQeBxt8iDueHro6LpeXcioAyMePUnQQ8ZzBN+Yt1pG
83fwqNMyHf8WIWutQvQw2CIbGORO2FaCx9XgL+Le9ENMJb7ZQwV13r7PuHAV/6V1
OwI/1Cn73cZ2uyWu8BHZbSqMctQsAkaT/pbPEUbrF4KB2GSigM+mux+Vkn9w3VK6
pNg5pUwCP0lqi9K1RNWEXyi4NQumrR+IEiaiV05twZ1oBaWBGXSTw12hIulZ3/v6
GLiwfk9I5mr7yDWVDdyCsTu1rhfen+Lp4ClyfWHISRPL1mko4W9leczgPWPz4pIp
AgMBAAGjUDBOMAwGA1UdEwQFMAMBAQEwHQYDVR0OBBYEFMI3a8MtjW1x6dPPJGaV
LhMF7bGKMB8GA1UdIwQYMBaAFDgZfHnVZvx+cXUthBhHi837Wfw1MA0GCSqGSIb3
DQEBCwUAA4IBAQCprzpoj6UaEG4eqLg2L3HqsvY73/XE8ytuZ9wDC3HodnmpezUX
48XwJPHFO7OGPGWZgsU2qX/Zp7yUXkVFSK4VnmnSzUtXNVlU0oWEEOzQLrpphksH
dcF8YNN/Y65KnhzIU784uHeFefUpPaE6yS5OSZboptZWVF9y1LoU3F7gN0UGvVG9
hflz5O0/KvmYd+6+Yrje+2lbHiJHNXLmOPiZyk9TBDknygBuU14IOWghQim3yks9
tKk8D38Vl85V5aG9nO4STjx5J8BtSl0x6wW3t9WwU5UC9geCROhZI1XRBafIoKkn
VSgHLpLTARtLikbbg/3SxpnW12msHvgLVasf
-----END
CERTIFICATE-----

1.126 libssh2 1.7.0

1.126.1 Available under license :

/* Copyright (c) 2004-2007 Sara Golemon <sarag@libssh2.org>
* Copyright (c) 2005,2006 Mikhail Gusarov <dottedmag@dottedmag.net>
* Copyright (c) 2006-2007 The Written Word, Inc.
* Copyright (c) 2007 Eli Fant <elifantu@mail.ru>
* Copyright (c) 2009-2014 Daniel Stenberg
* Copyright (C) 2008, 2009 Simon Josefsson
* All rights reserved.
*
* Redistribution and use in source and binary forms,
* with or without modification, are permitted provided
* that the following conditions are met:
*
* Redistributions of source code must retain the above
* copyright notice, this list of conditions and the
* following disclaimer.
*
* Redistributions in binary form must reproduce the above
* copyright notice, this list of conditions and the following
* disclaimer in the documentation and/or other materials
* provided with the distribution.
*
* Neither the name of the copyright holder nor the names
* of any other contributors may be used to endorse or
* promote products
derived from this software without
* specific prior written permission.

*
* THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND
* CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES,
* INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
* OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR
* CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING,
* BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
* SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
* INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
* WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
* NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
* USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY
* OF SUCH DAMAGE.
*/

1.127 zstd 1.33

1.127.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it. (Some other Free Software Foundation software is covered by
the GNU Lesser General Public License instead.) You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price.
Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which
gives you legal permission to copy,
distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of

running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you

distribute the same sections as part of a whole which is a work based
on the Program, the distribution of the whole must be on the terms of
this License, whose permissions for other licensees extend to the
entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest
your rights to work written entirely by you; rather, the intent is to
exercise the right to control the distribution of derivative or
collective works based on the Program.

In addition, mere aggregation of another work not based on the Program
with the Program (or with a work based on the Program) on a volume of
a storage or distribution medium does not bring the other work under
the scope of this License.

3. You may copy and distribute the Program (or a work based on it,
under Section 2) in object code or executable form under the terms of
Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable
source code, which must be distributed under the terms of Sections
1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three
years, to give any third party, for a charge no more than your
cost of physically performing source distribution, a complete
machine-readable copy of the corresponding source code, to be
distributed under the terms of Sections 1 and 2 above on a medium
customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer
to distribute corresponding source code. (This alternative is
allowed only for noncommercial distribution
and only if you
received the program in object code or executable form with such
an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for
making modifications to it. For an executable work, complete source
code means all the source code for all modules it contains, plus any
associated interface definition files, plus the scripts used to
control compilation and installation of the executable. However, as a
special exception, the source code distributed need not include
anything that is normally distributed (in either source or binary
form) with the major components (compiler, kernel, and so on) of the
operating system on which the executable runs, unless that component
itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under

any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE,
THERE IS NO WARRANTY
FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR
THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU
General Public License as published by
the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful,

but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License along
with this program; if not, write to the Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute
it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this
is what you want to do, use the GNU Lesser General
Public License instead of this License.
BSD License

For Zstandard software

Copyright (c) 2016-present, Facebook, Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification,
are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this
  list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice,
  this list of conditions and the following disclaimer in the documentation
  and/or other materials provided with the distribution.

* Neither the name Facebook nor the names of its contributors may be used to
  endorse or promote products derived from this software without specific
  prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

1.128 gdbm 1.12

1.128.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007, 2011 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for
software and other kinds of works.

The licenses for most software and other practical works are designed
to take away your freedom to share and change the works. By contrast,
the GNU General Public License is intended to guarantee your freedom to
share and change all versions of a program--to make sure it remains free
software for all its users. We, the Free Software Foundation, use the
GNU General Public License for most of our software; it applies also to
any other work released this way by its authors. You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that

patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays
"Appropriate Legal Notices"
to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other
than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing
those activities but
which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited

permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content,
constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users'
Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep
intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must
license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation
and its resulting copyright are not
used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License,

in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or
customer support for that product
model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge.
You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the

object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and
execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information
does not include a
requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for

unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included
in this License, to the extent
that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections
15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive
additional terms are considered "further
restrictions" within the meaning of section 10. If the Program as you
received it, or any part of it, contains a notice stating that it is
governed by this License along with a term that is a further
restriction, you may remove that term. If a license document contains
a further restriction but permits relicensing or conveying under this
License, you may add to a covered work material governed by the terms
of that license document, provided that the further restriction does
not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you
must place, in the relevant source files, a statement of the
additional terms that apply to those files, or a notice indicating
where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the
form of a separately written license, or stated as exceptions;
the above requirements apply either way.

8. Termination.

You
may not propagate or modify a covered work except as expressly
provided under this License. Any attempt otherwise to propagate or
modify it is void, and will automatically terminate your rights under
this License (including any patent licenses granted under the third
paragraph of section 11).

However, if you cease all violation of this License, then your
license from a particular copyright holder is reinstated (a)
provisionally, unless and until the copyright holder explicitly and
finally terminates your license, and (b) permanently, if the copyright
holder fails to notify you of the violation by some reasonable means
prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is
reinstated permanently if the copyright holder notifies you of the
violation by some reasonable means, this is the first time you have
received notice of violation of this License (for any work) from that
copyright holder, and you cure the violation prior to 30 days
after
your receipt of the notice.

Termination of your rights under this section does not terminate the
licenses of parties who have received copies or rights from you under
this License. If your rights have been terminated and not permanently

reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims

owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is

conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to
28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this
License, you have
permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer

of warranty and limitation of liability provided
above cannot be given local legal effect according to their terms,
reviewing courts shall apply local law that most closely approximates
an absolute waiver of all civil liability in connection with the
Program, unless a warranty or assumption of liability accompanies a
copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest
possible use to the public, the best way to achieve this is to make it
free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest
to attach them to the start of each source file to most effectively
state the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief
idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation, either version 3 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>
This program comes
with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, your program's commands might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school, if any, to sign a "copyright disclaimer" for the program, if necessary. For more information on this, and how to apply and follow the GNU GPL, see <http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License. But first, please read <http://www.gnu.org/philosophy/why-not-lgpl.html>.

1.129 psmisc 22.21

1.129.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not

covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those

sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program
(or a work based on it,
under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program
in object code or executable form with such
an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component

itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled
to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based
on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit
royalty-free redistribution of the Program by
all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute
software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies
a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals

of preserving the free status of all derivatives of our free software and
of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY
FOR THE PROGRAM, TO THE EXTENT PERMITTED
BY APPLICABLE LAW. EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES
PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED
OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS
TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE
PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING,
REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING
WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR
REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES,
INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING
OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED
TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY
YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER
PROGRAMS),
EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE
POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest
possible use to the public, the best way to achieve this is to make it
free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest
to attach them to the start of each source file to most effectively
convey the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) 19yy <name of author>

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation; either version
2 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19yy name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands
`show w' and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this is what you want to do, use the GNU Library General
Public License instead of this License.

1.130 pciutils 3.5.1

1.130.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it. (Some other Free Software Foundation software is covered by
the GNU Lesser General Public License instead.) You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price. Our General Public Licenses are designed
to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid
anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate to certain responsibilities for you if you
distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether
gratis or for a fee, you must give the recipients all the rights that
you have. You must make sure that they, too, receive or can get the
source code. And you must show them these terms so they know their
rights.

We protect your rights with two steps: (1) copyright the software, and
(2) offer you this license which gives you legal permission to copy,
distribute
and/or modify the software.

Also, for each author's protection and ours, we want to make certain
that everyone understands that there is no warranty for this free
software. If the software is modified by someone else and passed on, we

want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and

distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole
or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered
independent and separate works in
themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based
on it,
under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are

prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in
certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Program under this License
may add an explicit geographical distribution limitation excluding
those countries, so that distribution is permitted only in or among
countries not thus excluded. In such case, this License incorporates
the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions
of the General Public License from time to time. Such new versions will
be similar in spirit to the present version, but may differ in detail to
address new problems or concerns.

Each version is given a distinguishing version number. If the Program
specifies a version number
of this License which applies to it and "any
later version", you have the option of following the terms and conditions
either of that version or of any later version published by the Free
Software Foundation. If the Program does not specify a version number of
this License, you may choose any version ever published by the Free Software
Foundation.

10. If you wish to incorporate parts of the Program into other free
programs whose distribution conditions are different, write to the author
to ask for permission. For software which is copyrighted by the Free
Software Foundation, write to the Free Software Foundation; we sometimes
make exceptions for this. Our decision will be guided by the two goals
of preserving the free status of all derivatives of our free software and
of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY
FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW.
EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES
PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED
OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS
TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE
PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING,
REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING
WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR
REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES,
INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING

OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN
IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License,
or
(at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w'
and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this is what you want to do, use the GNU Lesser General
Public License instead of this License.

1.131 libsepol 2.6

1.131.1 Available under license :

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts
as the successor of the GNU Library Public License, version 2, hence
the version number 2.1.]

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
Licenses are intended to guarantee your freedom to share and change
free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some
specially designated software packages--typically libraries--of the
Free Software Foundation and other authors who decide to use it. You

can use it too, but we suggest
you first think carefully about whether
this license or the ordinary General Public License is the better
strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use,
not price. Our General Public Licenses are designed to make sure that
you have the freedom to distribute copies of free software (and charge
for this service if you wish); that you receive source code or can get
it if you want it; that you can change the software and use pieces of
it in new free programs; and that you are informed that you can do
these things.

To protect your rights, we need to make restrictions that forbid
distributors to deny you these rights or to ask you to surrender these
rights. These restrictions translate to certain responsibilities for
you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis
or for a fee, you must give the recipients
all the rights that we gave
you. You must make sure that they, too, receive or can get the source
code. If you link other code with the library, you must provide
complete object files to the recipients, so that they can relink them
with the library after making changes to the library and recompiling
it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the
library, and (2) we offer you this license, which gives you legal
permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that
there is no warranty for the free library. Also, if the library is
modified by someone else and passed on, the recipients should know
that what they have is not the original version, so that the original
author's reputation will not be affected by problems that might be
introduced by others.

Finally, software patents pose a constant threat to the existence
of
any free program. We wish to make sure that a company cannot
effectively restrict the users of a free program by obtaining a
restrictive license from a patent holder. Therefore, we insist that
any patent license obtained for a version of the library must be
consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the
ordinary GNU General Public License. This license, the GNU Lesser

General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits
its criteria of freedom. The Lesser General
Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use
the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without
limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish
on each copy an
appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a

fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License.
Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables
containing that work also fall under Section 6,
whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable
source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under

the terms of the
Sections above.

b) Give prominent notice with the combined library of the fact
that part of it is a work based on the Library, and explaining
where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing
the Library (or any work based on the
Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute
so as to satisfy simultaneously your obligations under this
License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any

particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of

all derivatives of our free software and of promoting the sharing
and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL
DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line
and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or
modify it under the terms of the GNU Lesser General Public

License as published by the Free Software Foundation; either
version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public
License along with this library; if not, write to the Free Software
Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should
also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the library, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the
library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

1.132 flex 2.6.0

1.132.1 Available under license :

Flex carries the copyright used for BSD software, slightly modified
because it originated at the Lawrence Berkeley (not Livermore!) Laboratory,
which operates under a contract with the Department of Energy:

Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006, 2007 The Flex Project.

Copyright (c) 1990, 1997 The Regents of the University of California.
All rights reserved.

This code is derived from software contributed to Berkeley by
Vern Paxson.

The United States Government has rights in this work pursuant
to contract no. DE-AC03-76SF00098 between the United States
Department of Energy and the University of California.

Redistribution and use in source and binary forms, with or without

modification, are permitted provided that the following conditions
are met:

1. Redistributions of source code must retain the above copyright
  notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions
 and the following disclaimer in the
  documentation and/or other materials provided with the distribution.

Neither the name of the University nor the names of its contributors
may be used to endorse or promote products derived from this software
without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE.

This basically says "do whatever you please with this software except
remove this notice or take advantage of the University's (or the flex
authors') name".

Note that the "flex.skl" scanner skeleton carries no copyright notice.
You are free to do whatever you please with scanners generated using flex;
for them, you are not even bound by the above copyright.

1.133 efibootmgr 0.12

1.134 libsemanage-common 2.6

1.134.1 Available under license :

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts
as the successor of the GNU Library Public License, version 2, hence
the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest
you first think carefully about whether
this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients
all the rights that we gave
you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence

of
any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits
its criteria of freedom. The Lesser General
Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use
the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the

users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without
limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that

you conspicuously and appropriately publish
on each copy an
appropriate copyright notice and disclaimer of warranty; keep intact
all the notices that refer to this License and to the absence of any
warranty; and distribute a copy of this License along with the
Library.

You may charge a fee for the physical act of transferring a copy,
and you may at your option offer warranty protection in exchange for a
fee.

2. You may modify your copy or copies of the Library or any portion
of it, thus forming a work based on the Library, and copy and
distribute such modifications or work under the terms of Section 1
above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices
stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no
charge to all third parties under the terms of this License.

d) If a facility in the modified
Library refers to a function or a
table of data to be supplied by an application program that uses
the facility, other than as an argument passed when the facility
is invoked, then you must make a good faith effort to ensure that,
in the event an application does not supply such function or
table, the facility still operates, and performs whatever part of
its purpose remains meaningful.

(For example, a function in a library to compute square roots has
a purpose that is entirely well-defined independent of the
application. Therefore, Subsection 2d requires that any
application-supplied function or table used by this function must
be optional: if the application does not supply it, the square
root function must still compute square roots.)

These requirements apply to the modified work as a whole. If
identifiable sections of that work are not derived from the Library,
and can be reasonably considered independent and separate works in
themselves,
then this License, and its terms, do not apply to those
sections when you distribute them as separate works. But when you
distribute the same sections as part of a whole which is a work based
on the Library, the distribution of the whole must be on the terms of

this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a

work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License.
Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables
containing that work also fall under Section 6,
whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable

source code for the Library including whatever
changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user
installs one, as long as the modified version is
interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major
components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot

distribute
so as to satisfy simultaneously your obligations under this
License and any other pertinent obligations, then as a consequence you
may not distribute the Library at all. For example, if a patent
license would not permit royalty-free redistribution of the Library by
all those who receive copies directly or indirectly through you, then
the only way you could satisfy both it and this License would be to
refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any
particular circumstance, the balance of the section is intended to apply,
and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any
patents or other property right claims or to contest validity of any
such claims; this section has the sole purpose of protecting the
integrity of the free software distribution system which is
implemented by public license practices. Many people
have made
generous contributions to the wide range of software distributed
through that system in reliance on consistent application of that
system; it is up to the author/donor to decide if he or she is willing
to distribute software through any other system and a licensee cannot
impose that choice.

This section is intended to make thoroughly clear what is believed to
be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in
certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Library under this License may add
an explicit geographical distribution limitation excluding those countries,
so that distribution is permitted only in or among countries not thus
excluded. In such case, this License incorporates the limitation as if
written in the body of this License.

13. The Free Software Foundation may publish revised and/or new
versions of the Lesser General Public
License from time to time.
Such new versions will be similar in spirit to the present version,
but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library
specifies a version number of this License which applies to it and
"any later version", you have the option of following the terms and
conditions either of that version or of any later version published by
the Free Software Foundation. If the Library does not specify a
license version number, you may choose any version ever published by

the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively

convey the exclusion of warranty; and each file should have at least the
"copyright" line
and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or
modify it under the terms of the GNU Lesser General Public
License as published by the Free Software Foundation; either
version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public
License along with this library; if not, write to the Free Software
Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should
also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the library, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the
library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

1.135 libedit 20150325-3.1

1.135.1 Available under license :

Copyright (c) 1992, 1993
The Regents of the University of California. All rights reserved.

This code is derived from software contributed to Berkeley by
Christos Zoulas of Cornell University.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions

are met:
1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors
may be used to endorse or promote products derived from this software
without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

1.136 dmidecode 3.5

1.136.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it. (Some other Free Software Foundation software is covered by
the GNU Lesser General Public License instead.) You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not

price.

Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which
gives you legal permission to copy,
distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it,

either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a

special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source
code, even though third parties are not
compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing
or modifying
the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For

example, if a patent
license would not permit royalty-free redistribution of the Program by
all those who receive copies directly or indirectly through you, then
the only way you could satisfy both it and this License would be to
refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under
any particular circumstance, the balance of the section is intended to
apply and the section as a whole is intended to apply in other
circumstances.

It is not the purpose of this section to induce you to infringe any
patents or other property right claims or to contest validity of any
such claims; this section has the sole purpose of protecting the
integrity of the free software distribution system, which is
implemented by public license practices. Many people have made
generous contributions to the wide range of software distributed
through that system in reliance on consistent application of that
system; it is up to the author/donor to
decide if he or she is willing
to distribute software through any other system and a licensee cannot
impose that choice.

This section is intended to make thoroughly clear what is believed to
be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in
certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Program under this License
may add an explicit geographical distribution limitation excluding
those countries, so that distribution is permitted only in or among
countries not thus excluded. In such case, this License incorporates
the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions
of the General Public License from time to time. Such new versions will
be similar in spirit to the present version, but may differ in detail to
address new problems or concerns.

Each version is given a distinguishing
version number. If the Program
specifies a version number of this License which applies to it and "any
later version", you have the option of following the terms and conditions
either of that version or of any later version published by the Free
Software Foundation. If the Program does not specify a version number of
this License, you may choose any version ever published by the Free Software
Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU
General Public License as published by
the Free Software Foundation; either version 2 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License along
with this program; if not, write to the Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute
it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this
is what you want to do, use the GNU Lesser General
Public License instead of this License.

1.137 pinentry 0.9.2

1.137.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
675 Mass Ave, Cambridge, MA 02139, USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed
to make sure that you
have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute

and/or modify the software.

Also, for each author's protection and ours, we want to make certain
that everyone understands that there is no warranty for this free
software. If the software is modified by someone else and passed on, we
want its recipients to know that what they have is not the original, so
that any problems introduced by others will not reflect on the original
authors' reputations.

Finally, any free program is threatened constantly by software
patents. We wish to avoid the danger that redistributors of a free
program will individually obtain patent licenses, in effect making the
program proprietary. To prevent this, we have made it clear that any
patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and
modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work
which contains
a notice placed by the copyright holder saying it may be distributed
under the terms of this General Public License. The "Program", below,
refers to any such program or work, and a "work based on the Program"
means either the Program or any derivative work under copyright law:
that is to say, a work containing the Program or a portion of it,
either verbatim or with modifications and/or translated into another
language. (Hereinafter, translation is included without limitation in
the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not
covered by this License; they are outside its scope. The act of
running the Program is not restricted, and the output from the Program
is covered only if its contents constitute a work based on the
Program (independent of having been made by running the Program).
Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim
copies of the Program's
source code as you receive it, in any medium, provided that you
conspicuously and appropriately publish on each copy an appropriate
copyright notice and disclaimer of warranty; keep intact all the
notices that refer to this License and to the absence of any warranty;
and give any other recipients of the Program a copy of this License
along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole
or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably
considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such

parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6.
Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free
redistribution of the Program by
all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through

any other system and a licensee cannot
impose that choice.

This section is intended to make thoroughly clear what is believed to
be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in
certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Program under this License
may add an explicit geographical distribution limitation excluding
those countries, so that distribution is permitted only in or among
countries not thus excluded. In such case, this License incorporates
the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions
of the General Public License from time to time. Such new versions will
be similar in spirit to the present version, but may differ in detail to
address new problems or concerns.

Each version is given a distinguishing version number. If the Program
specifies a version number
of this License which applies to it and "any
later version", you have the option of following the terms and conditions
either of that version or of any later version published by the Free
Software Foundation. If the Program does not specify a version number of
this License, you may choose any version ever published by the Free Software
Foundation.

10. If you wish to incorporate parts of the Program into other free
programs whose distribution conditions are different, write to the author
to ask for permission. For software which is copyrighted by the Free
Software Foundation, write to the Free Software Foundation; we sometimes
make exceptions for this. Our decision will be guided by the two goals
of preserving the free status of all derivatives of our free software and
of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY
FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE
LAW. EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES
PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED
OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS
TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE
PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING,
REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS),
EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

1.138 berkeley-db 6.0.35

1.138.1 Available under license :

GNU AFFERO GENERAL PUBLIC LICENSE
Version 3, 19 November 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU Affero General Public License is a free, copyleft license for software and other kinds of works, specifically designed to ensure cooperation with the community in the case of network server software.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works.
By contrast,
our General Public Licenses are intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

Developers that use our General Public Licenses protect your rights with two

steps: (1) assert copyright on the software, and (2) offer
you this License which gives you legal permission to copy, distribute
and/or modify the software.

A secondary benefit of defending all users' freedom is that
improvements made in alternate versions of the program, if they
receive widespread use, become available for other developers to
incorporate. Many developers of free software are heartened and
encouraged by the resulting cooperation. However, in the case of
software used on network servers, this result may fail to come about.
The GNU General Public License permits making a modified version and
letting the public access it on a server without ever releasing its
source code to
the public.

The GNU Affero General Public License is designed specifically to
ensure that, in such cases, the modified source code becomes available
to the community. It requires the operator of a network server to
provide the source code of the modified version running there to the
users of that server. Therefore, public use of a modified version, on
a publicly accessible server, gives the public access to the source
code of the modified version.

An older license, called the Affero General Public License and
published by Affero, was designed to accomplish similar goals. This is
a different license, not a version of the Affero GPL, but Affero has
released
a new version of the Affero GPL which permits relicensing under
this license.

The precise terms and conditions for copying, distribution and
modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU Affero General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of
works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this
License. Each licensee is addressed as "you". "Licensees" and
"recipients" may be individuals
or organizations.

To "modify" a work means to copy from or adapt all or part of the work

in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying,

distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License,
and how to view a copy of this License. If
the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System
Libraries" of an executable work include anything, other
than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component

(kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section

7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not

used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical

medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this

conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the

Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being
offered to the general public at no
charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a

typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent

the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by

this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining
to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further

restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does

not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions;
the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright

holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently

reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However,

nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of

this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory

patent license (a) in connection with copies of the covered work

conveyed by you (or copies made from those copies), or (b) primarily
for and in connection with specific products or compilations that
contain the covered work, unless you entered into that arrangement,
or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting
any implied license or other defenses to infringement that may
otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or
otherwise) that contradict the conditions of this License, they do not
excuse you from the conditions
of this License. If you cannot convey a
covered work so as to satisfy simultaneously your obligations under this
License and any other pertinent obligations, then as a consequence you may
not convey it at all. For example, if you agree to terms that obligate you
to collect a royalty for further conveying from those to whom you convey
the Program, the only way you could satisfy both those terms and this
License would be to refrain entirely from conveying the Program.

13. Remote Network Interaction; Use with the GNU General Public License.

Notwithstanding any other provision of this License, if you modify the
Program, your modified version must prominently offer all users
interacting
with it remotely through a computer network (if your version
supports such interaction) an opportunity to receive the Corresponding
Source of your version by providing access to the Corresponding Source
from a network server at no charge, through some standard or customary
means of facilitating copying of software. This Corresponding Source
shall include the Corresponding Source for any work covered by version 3
of the GNU General Public License that is incorporated pursuant to the
following paragraph.

Notwithstanding any other provision of this License, you have
permission to link or combine any covered work with a work licensed
under version 3 of the GNU General Public License into a single

combined work, and to convey the resulting work. The terms of this
License will continue to apply to the part which is the covered work,
but the work with which it is combined will remain governed by version
3 of the GNU General Public License.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU Affero General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU Affero General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU Affero General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU Affero General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY

OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR

PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM

IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS

THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY

GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE

USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF

DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD

PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS),

EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED
OF THE POSSIBILITY OF
SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided
above cannot be given local legal effect according to their terms,
reviewing courts shall apply local law that most closely approximates
an absolute waiver of all civil liability in connection with the
Program, unless a warranty or assumption of liability accompanies a
copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program,
and you want it to be of the greatest
possible use to the public, the best way to achieve this is to make it
free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest
to attach them to the start of each source file to most effectively
state the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify
it under
the terms of the GNU Affero General Public License as published by
the Free Software Foundation, either version 3 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the

GNU Affero General Public License for more details.

You should have received a copy of the GNU Affero General Public License along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If your software can interact with users remotely through a computer network, you should also make sure that it provides a way for users to get its source. For example, if your program is a web application, its interface could display a "Source" link that leads users to an archive of the code. There are many ways you could offer source, and different solutions will be better for different programs; see section 13 for the specific requirements.

You should also get your employer (if you work as a programmer) or school, if any, to sign a "copyright disclaimer" for the program, if necessary. For more information on this, and how to apply and follow the GNU AGPL, see <http://www.gnu.org/licenses/>.

1.139 npth 1.2

1.139.1 Available under license :

GNU LESSER GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and the "GNU GPL" refers to version 3 of the GNU General Public License.

"The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An "Application" is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library.

Defining a subclass of a class defined by
the Library is deemed a mode
of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters,
data structure
layouts and accessors, or small macros, inline functions and templates

(ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide

whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain
that everyone understands that there is no warranty for this free
software. If the software is modified by someone else and passed on, we
want its recipients to know that what they have is not the original, so
that any problems introduced by others will not reflect on the original
authors' reputations.

Finally, any free program is threatened constantly by software
patents. We wish to avoid the danger that redistributors of a free
program will individually obtain patent licenses, in effect making the
program proprietary. To prevent this, we have made it clear that any
patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and
modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which
contains
a notice placed by the copyright holder saying it may be distributed
under the terms of this General Public License. The "Program", below,
refers to any such program or work, and a "work based on the Program"
means either the Program or any derivative work under copyright law:
that is to say, a work containing the Program or a portion of it,
either verbatim or with modifications and/or translated into another
language. (Hereinafter, translation is included without limitation in
the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not
covered by this License; they are outside its scope. The act of
running the Program is not restricted, and the output from the Program
is covered only if its contents constitute a work based on the
Program (independent of having been made by running the Program).
Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies
of the Program's
source code as you receive it, in any medium, provided that you
conspicuously and appropriately publish on each copy an appropriate
copyright notice and disclaimer of warranty; keep intact all the
notices that refer to this License and to the absence of any warranty;
and give any other recipients of the Program a copy of this License
along with the Program.

You may charge a fee for the physical act of transferring a copy, and
you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole
or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered
independent and separate works in
themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based

on it,
under Section 2) in object code or executable form under the terms of
Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable
source code, which must be distributed under the terms of Sections
1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three
years, to give any third party, for a charge no more than your
cost of physically performing source distribution, a complete
machine-readable copy of the corresponding source code, to be
distributed under the terms of Sections 1 and 2 above on a medium
customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer
to distribute corresponding source code. (This alternative is
allowed only for noncommercial distribution and only if you
received the program in object code or
executable form with such
an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for
making modifications to it. For an executable work, complete source
code means all the source code for all modules it contains, plus any
associated interface definition files, plus the scripts used to
control compilation and installation of the executable. However, as a
special exception, the source code distributed need not include
anything that is normally distributed (in either source or binary
form) with the major components (compiler, kernel, and so on) of the
operating system on which the executable runs, unless that component
itself accompanies the executable.

If distribution of executable or object code is made by offering
access to copy from a designated place, then offering equivalent
access to copy the source code from the same place counts as
distribution of the source code, even though third parties are not
compelled to copy the
source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program
except as expressly provided under this License. Any attempt
otherwise to copy, modify, sublicense or distribute the Program is
void, and will automatically terminate your rights under this License.
However, parties who have received copies, or rights, from you under
this License will not have their licenses terminated so long as such
parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to
be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in
certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Program under this License
may add an explicit geographical distribution limitation excluding
those countries, so that distribution is permitted only in or among
countries not thus excluded. In such case, this License incorporates
the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions
of the General Public License from time to time. Such new versions will
be similar in spirit to the present version, but may differ in detail to
address new problems or concerns.

Each version is given a distinguishing version number. If the Program
specifies a version number
of this License which applies to it and "any
later version", you have the option of following the terms and conditions
either of that version or of any later version published by the Free
Software Foundation. If the Program does not specify a version number of
this License, you may choose any version ever published by the Free Software
Foundation.

10. If you wish to incorporate parts of the Program into other free
programs whose distribution conditions are different, write to the author
to ask for permission. For software which is copyrighted by the Free
Software Foundation, write to the Free Software Foundation; we sometimes
make exceptions for this. Our decision will be guided by the two goals
of preserving the free status of all derivatives of our free software and
of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY
FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW.
EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES
PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED
OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS
TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE
PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING,
REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING

WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN
IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.

This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w'
and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this is what you want to do, use the GNU Lesser General
Public License instead of this License.
GNU LESSER GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates
the terms and conditions of version 3 of the GNU General Public
License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, "this License" refers to version 3 of the GNU Lesser
General Public License, and the "GNU GPL" refers to version 3 of the GNU
General Public License.

"The Library" refers to a covered work governed by this License,
other than an Application or a Combined Work as defined below.

An "Application" is any work that makes use of an interface provided
by the Library, but which is not otherwise based on the Library.
Defining a subclass of a class defined by the Library is

deemed a mode
of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying
Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data
structure
layouts and accessors, or small macros, inline functions and templates

(ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide

whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

1.140 hd-parm 9.56

1.140.1 Available under license :

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public
Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and
(2) offer you this license which gives you legal permission
to copy,
distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain
that everyone understands that there is no warranty for this free
software. If the software is modified by someone else and passed on, we
want its recipients to know that what they have is not the original, so
that any problems introduced by others will not reflect on the original
authors' reputations.

Finally, any free program is threatened constantly by software
patents. We wish to avoid the danger that redistributors of a free
program will individually obtain patent licenses, in effect making the
program proprietary. To prevent this, we have made it clear that any
patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and
modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program
or other work which contains
a notice placed by the copyright holder saying it may be distributed
under the terms of this General Public License. The "Program", below,
refers to any such program or work, and a "work based on the Program"
means either the Program or any derivative work under copyright law:
that is to say, a work containing the Program or a portion of it,
either verbatim or with modifications and/or translated into another
language. (Hereinafter, translation is included without limitation in
the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not
covered by this License; they are outside its scope. The act of
running the Program is not restricted, and the output from the Program
is covered only if its contents constitute a work based on the
Program (independent of having been made by running the Program).
Whether that is true depends on what the Program does.

1. You may copy and distribute
verbatim copies of the Program's
source code as you receive it, in any medium, provided that you
conspicuously and appropriately publish on each copy an appropriate
copyright notice and disclaimer of warranty; keep intact all the

notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt

otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based
on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit
royalty-free redistribution of the Program by
all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made

generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute
software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies
a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED
BY APPLICABLE LAW. EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF

MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER
PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version
2 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

  Gnomovision version 69, Copyright (C) year name of author
  Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
  This is free software, and you are welcome to redistribute it
  under certain conditions; type `show c' for details.

The hypothetical
 commands `show w' and `show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

 Yoyodyne, Inc., hereby disclaims all copyright interest in the program
 `Gnomovision' (which makes passes at compilers) written by James Hacker.

 <signature of Ty Coon>, 1 April 1989
 Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this is what you want to do, use the GNU Library General
Public License instead of this License.
BSD-Style Open Source License:

You may freely use, modify, and redistribute the hdparm program,
as either binary or source, or both.

The only condition is that my name and copyright notice
remain in the source code as-is.

The apt.c file is Copyright (c) 2009 Jan Friesse <jfriesse@gmail.com>.
You may use/distribute apt.c freely, under the terms of either
(your choice) the GNU General Public License version 2,
or a BSD style license.

Mark Lord (mlord@pobox.com)
This package was debianized by Christopher L Cheney <ccheney@debian.org> on
Wed, 21 Nov 2001 15:51:14 -0600.

It was downloaded from http://www.ibiblio.org/pub/Linux/system/hardware

Upstream Author: Mark S. Lord <mlord@pobox.com>

Copyright:

/* hdparm.c - Command line interface to get/set hard disk parameters */
/*   - by Mark Lord 1994-2008 -- freely distributable */

You are free to distribute this software under the terms of the BSD License.
On Debian systems, the complete text of the BSD License can be found in
/usr/share/common-licenses/BSD

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries.To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

©2024 Cisco Systems, Inc. All rights reserved.